HARRAN ÜNİVERSİTESİ MÜHENDİSLİK FAKÜLTESİ
AKADEMİK BİLİM DERGİSİ

HARRAN ÜNİVERSİTESİ MÜHENDİSLİK DERGİSİ

HARRAN UNIVERSITY JOURNAL OF ENGINEERING

e-ISSN: 2528-8733

HARRAN ÜNİVERSİTESİ MÜHENDİSLİK DERGİSİ

HARRAN UNIVERSITY JOURNAL of ENGINEERING

e-ISSN: 2528-8733 (ONLINE)
URL: http://dergipark.gov.tr/humder

A Comprehensive Review About Image Encryption Methods

Görüntü Şifreleme Yöntemlerinin Kapsamlı Bir İncelemesi

Yazar(lar) (Author(s)): *Cihan TİKEN[1], Rüya ŞAMLI[2]*

[1] ORCID ID: 0000-0001-7844-2579
[2] ORCID ID: 0000-0002-8723-1228

Bu makaleye şu şekilde atıfta bulunabilirsiniz (To cite to this article): Tiken C., Samli R., "A Comprehensive Review About Image Encryption Methods", ***Harran Üniversitesi Mühendislik Dergisi***, 7(1): 27-49, (2022).

Erişim linki (To link to this article): http://dergipark.gov.tr/humder/archive

HRU Muh Der, 7(1): 27-49 (2022)

Harran Üniversitesi

Mühendislik Dergisi

http://dergipark.gov.tr/humder

Derleme Makalesi

A Comprehensive Review About Image Encryption Methods

Cihan TİKEN[1,2]*, Rüya ŞAMLI[2]

[1]*Harran University, 63200, Haliliye/ŞANLIURFA*

[2]*Department of Computer Engineering, Faculty of Engineering, İstanbul University-Cerrahpasa, 34320, Avcılar/İstanbul*

Makale Bilgisi

Başvuru: 01/02/2022
Yayın:30/04/2022

Keywords

Data security
Cryptology
Image processing
Steganography

Anahtar Kelimeler

Veri güvenliği
Kriptoloji
Görüntü işleme
Steganografi

Abstract

In today’s technology world, data security has a great importance. Because each data type has its own characteristics, there are various methods of providing this security. The main subject of this study is the security of image data which are more complex structures than text data. Using traditional encryption methods alone to ensure security in image data types can create security weaknesses. For this reason, nowadays, some traditional methods are combined with each other or different methods to encrypt image data. In this study, 131 articles were examined and image encryption methods were classified according to the traditional methods, some new methods or combinations of some methods, that they contain. Studies on both colored and gray level images have been handled together. Finally, the images used in the articles were compared with each other in many ways and the results were presented graphically.

Görüntü Şifreleme Yöntemlerinin Kapsamlı Bir İncelemesi

Öz

Günümüz teknoloji dünyasında veri güvenliği büyük önem taşımaktadır. Her veri türünün kendine has özellikleri olduğu için bu güvenliği sağlamanın çeşitli yöntemleri vardır. Bu çalışmanın ana konusu, metin verilerinden daha karmaşık yapılar olan görüntü verilerinin güvenliğidir. Görüntü veri türlerinde güvenliği sağlamak için tek başına geleneksel şifreleme yöntemlerini kullanmak güvenlik zafiyetleri yaratabilir. Bu nedenle günümüzde görüntü verilerini şifrelemek için bazı geleneksel yöntemler birbiriyle veya farklı yöntemler ile birleştirilmektedir. Bu çalışmada 131 makale incelenmiş ve görüntü şifreleme yöntemleri içerdikleri geleneksel yöntemlere, bazı yeni yöntemlere veya bazı yöntemlerin kombinasyonlarına göre sınıflandırılmıştır. Hem renkli hem de gri seviyeli görüntüler üzerinde yapılan çalışmalar birlikte ele alınmıştır. Son olarak makalelerde kullanılan görseller birçok yönden birbirleriyle karşılaştırılmış ve sonuçlar grafiksel olarak sunulmuştur.

1. INTRODUCTION

In recent days, transmission of data in a safe and concealed mood by using different manners is crucial, because communication over open networks is becoming more frequent. The rapid development of Internet technologies nominated multimedia techniques during communication as dominant methods of communication. [1]. This makes data protection as an important concern for individuals and organizations and also online data privacy becomes an important research area. There are many data protection techniques such as encryption including conventional encryptions and steganography. Although encryption aims to prevent unauthorized access by scrambling data, the main purpose of steganography is to hide data in a recipient / cover object so that it can be hidden [2].

After encrypting text files, it is easy to processing, storing and sending via a network these encrypted files. Because of huge data size, complexity and some real time constraints encryption of multimedia data becomes more difficult. Since this is the case some different techniques such as chaos based, Genetic Algorithm (GA) and Least Significant Bit (LSB) are more attractive than traditional encryption schemes

*İletişim yazarı, e-mail: ctiken@harran.edu.tr

[3]. There is a summary about different studies which are contain different image encryption methods below.

The researchers proposed a novel image cryptography technique which is an extremely powerful method based on principle of Rubik's cube in [4]. Principle of Rubik's cube and a digital chaotic key are used in synchronized way in this technique. So, this technique provides a secret image whichs pixels are mixed, XOR operator is implemented to columns and rows of the mixed image. A chaos based cipher is used for this process. In [5], to improve the security and stability of the encryption algorithms which have a permutation-diffusion structure, a new image encryption method is proposed by using Coupled-Map Lattices (CML) and a fractional-order chaotic system together. According to proposed method's results this technique provides a stability versus geometric attacks and several image processing actions.

Authors in [6,7] proposed two different LSB based steganographic techniques. In the first one, an adaptive LSB substitution method which uses uncorrelated color space is used to minimize the possibility of recognition by human eyes while rising the imperceptibility feature. In the second one a method which turns Red, Green, and Blue (RGB) color space images to Hue-Saturation-Intensity (HSI) color space, hides the data into Intensity Plane (I-Plane) and then turn it to RGB color model after hiding is proposed.

Discrete Cosine Transform (DCT) is an another image encryption method. In [8], DCT and Discrete Wavelet Transform (DWT) digital image transformation techniques are combined to suggest a new digital images encryption method for Wireless Sensor Networks (WSN).

GA based method proposed in [9] does not allow loss of data but allows an adjustable visual image quality in spatial domain. The basic concept of this technique is forming the steganography problem as an optimization and search problem and encrypting a secret image into 'n' specious shadows is called Secret Image Sharing (SIS) scheme. If any part of the shadows is not obtained it is not possible to reach any part of data on the secret image. In [10], encrypted shadow images using optimal Homomorphic Encryption (HE) technique is proposed with wavelet-based secret image sharing scheme. Initially, to procure sub bands, DWT is implemented on the secret image. By doing this operation for each shadows various shadows are built, encrypted and decrypted. HE technique is used to each shadow's encryption and decryption, to increase security of shadow.

As can be seen from the reviewed articles, many different methods show success about image encryption security and data integrity.

The rest of the paper is organized as follows: In Section II, image encryption concept and used methods during encryption are briefly mentioned. Section III presents a categorizing of image encryption methods and briefs of some papers which have utilized these techniques. Section IV reveals the results and discussion of handled studies by using specified comparison metrics. The study is concluded in Section V.

2. IMAGE ENCRYPTION

The digital images are the raw materials of image processing and they are consisting of a number of "pixels", which are made up regulation of some numbers which are symbolize light intensities. These pixels can be assumed as small dots on the screen and digital images are formed by combination of these dots. Image features can be understood from these pixels [11].

Nowadays there are many crucial fields that image informations are shared such as electronic commerce, military, medicine, education, aerospace and so on. [12]. There are two main purposes of encryption: (i) storing data in a secure manner, (ii) transmitting data confidentially over the network. As it is known, network attacks are increasing day by day by using new techniques. Due to the characteristics and importance of digital image and to avoid attacks from any unauthorized people/company/system and so on, many different preventive techniques and approaches have been developed to make data over a network confidential and durable and also storing data in secret [13]. These techniques are based on chaos [14, 15], DCT [16, 17], GA [18, 19], XOR operations [20, 21] and Neural Networks (NN) [22, 23].

3. IMAGE ENCRYPTION TECHNIQUES

Currently, security of the data has become highly major matter because of increase of elevated demand in digital transmission and big loses depending to unauthorized access to overcome these issues and to provide safe data and to avoid unauthorized access, encryption is used. The traditional encryption schemes are suitable only for encrypting text data, and certain defects exist in the current schemes used to encode video streams and images to handle this issue, a plenty of image encryption algorithms have been proposed [24]. In this study, some image encryption techniques have been classified based on their main encryption schemes that is used during encryption and then these main schemes will be reviewed shortly.

3.1. Chaos Based Methods

In the image encryption field, the number of chaos-based methods is quite large. The main reason of this abundance is some perfect properties of chaotic systems. Some chaos based studies are handled below.

A four-dimensional chaotic system based rapid encryption method which works on colored images is proposed in [25]. This study's aim is to improve the complexity and key space of classical equations of three-dimensional chaotic system so first of all, a four-dimensional chaotic system is designed by improving the three-dimensional chaotic system. As the second step, to obtain a better image encryption speed, a new pseudo-random sequence generator is designed, because the characteristic of colored images' pixels' channel requires this. Finally, for distribution of the main image, the row-major and column-major techniques are used. Also by using the cat map with parameter, scrambling of image pixels is provided. By doing this an efficiency of encryption is obtained. Experimental results show good result in the sense of robustness, security and high encryption speed.

In [26], by using chaotic Amplitude Phase Frequency Model (APFM), a new nonlinear adaptive filter is proposed for colored images. For generating chaos, simulated time intervals, initial values and nine parameters are sent to APFM nonlinear adaptive filter. The plain image (colored image) could be encrypted and turn into cipher image that the RGB components are nearly distributed in an appropriate order. The method has an effective key sensitivity to take care of color image. The proposed method can successfully pass National Institute of Standards and Technology (NIST) SP 800-22a tests (cryptographic system secure tests). The result of experiments presents a good performance of security.

The simple but efficient chaotic system proposed in [27] combines two 1D chaotic maps (seed maps). With respect to performance assessment and the simulation results this method has ability to produce many 1D chaotic maps which have larger chaotic ranges and also preferable chaotic attitudes according to their seed maps. Every time this method implemented to the same original image. Then it can produce exactly different encrypted image each time.

In [28], a novel cryptographic algorithm which uses a two-dimensional and logistic chaotic economic map. The power of the method is indicated by applying this method on different types of images. By using statistical analyses like pixels' correlation, the entropy process, sensitivity to the key space, and contrast analysis, the application of the proposed method and its safety are analyzed. Experimental results present that this method withstands against differential, brute-force, noise and statistical attacks.

A new advanced hyperchaotic sequences based image encryption technique is proposed in [29]. At the beginning, to create chaotic key stream which is more appropriate to encrypt images, the hyperchaotic sequences are reformed. As the next step, to associate plaintext and the chaotic key stream that provide tenderness for both key and plaintext, the final encryption key stream is produced. A high sensitivity of key and plaintext is obtained during just two rounds diffusion operation. Best known security analysis and the performance tests have been applied. As a result, this method is determined as adoptable for the secure image communication applications.

In [30],a combination of complex Lorenz systems and complex Chen systems based colored image encryption method is suggested. According to real chaotic systems, the larger chaotic ranges and complex chaotic systems which has more complex behaviors could increase the security and extend key space of colored image encryption. This approach consists of three steps. In permutation process which is the initial step secret image's pixels are mixed between RGB channels individually by using two-dimensional and one-dimensional permutation. In the second step called diffusion process, to hide pixel information the XOR operation is used. Finally, to obtain a multilevel encryption RGB channels are mixed.

In [31], a novel chaotic economic map based image encryption algorithm is proposed. The proposed method is applied on a chaotic map based plain image. According to the results images are encrypted and decrypted successfully by using the same security keys. Security analysis reveal very good results in terms of information entropy.

In [32], an image cryptography with Matrix Array Symmetric Key (MASK) is proposed using chaos based approach. In [33], an image encryption by chaos mixing method is proposed. Chaos based edge adaptive image steganography has been presented in [34]. A novel colored image encryption algorithm based on chaos presented in [35]. In [36], a new hyper-chaotic circuit which includes two memristors is handled, also there is application that is obtained by applying the proposed method. A chaotic logistic map based technique is used in [37].

In [38], One-Way Coupled-Map Lattices (OCML) based image encryption method proposed owing to their hyper-chaotic behaviors. By using Chaotic Random Phase Mask (CRPM) a fully phase multiple-image encryption is presented in [39]. A new approach for data hiding which uses chaotic map is proposed in [40]. A hyper-chaotic system and chaotic control parameters based robust hybrid image encryption algorithm is proposed in [41]. In [42], the most important component of image encryption which are secret keys are generated from a spatiotemporal chaotic system. 1D logistic map to make fast encryption process is proposed in [43]. As seen from these studies, chaos based encryption methods has a large share at image encryption area.

3.2. Neural Network (NN) Based Methods

Neurons in the human neural system combine thousands of temporal signals owing to their dendrites. Internal potential of these signals are changed in a complicated way by signals itself. This change is based on stimulant or restrictive nature of the synapses. A NN has a directed graph topology which represents a highly parallelized dynamic system. The groups of artificial neurons which are connected to each other usually adjusted into layers, sublayers or fields embody NNs. The behavior of such groups alter depend on changes in architectures and also neuron signal functions. Neurons are basic non-linear computing elements; NNs are parallel adaptive networks of neurons. These neurons are designed to act as a human neuron and actualize some properties of human nervous system [44]. NNs based researches are reviewed in this part.

In [45], a new technique is improved to assimilate deep NNs within the convenient restriction of available homomorphic encryption schemes. Authors especially deals on classification of the notable Convolutional Neural Networks (CNN). A method has been designed for approach of activation functions such as Tanh, ReLU and Sigmoid which are well-known in CNNs. Then these approximate values are used in place of original activation functions after that model’s performance is analyzed. At the end CNNs are applied over encrypted data and efficiency of the model has been measured.

In [46], homomorphic encryption is used for confidentiality of requirements, encrypted data is sent by sender to third party that use a trained model to get a prediction. The model sends back an encrypted prediction to the sender after working on cipher texts. In this study the predicted value and the original data are both in secure and only data owner can reach this data. This study shows that a safe cloud based NNs prediction services can be formed. and also it ensures privacy of millions users.

In [47], there are four new notions presented by the authors. Firstly, steganography which generally uses a single cover data to hide the secret data. But authors present a new method using remote sensing image which is called "multi-cover steganography". Satellites take three shots as remote sensing images, combination of these three images creates a false colored image. Secondly, an approach has been intended to overcome the problem of exchange of secret keys via network this is called general recursion neural cryptosystem. Thirdly, the keys are exchanged through trine network to be used to decrypt the data. This strong cryptosystem combine to the multi-cover steganography. Finally, by using LSB algorithm an irregular encoding method is designed. This new encoding procedure confirms the confidence of the secret data.

In [48], deep learning which is one of the popular types of NNs is used as the feature classification on the iris images. The common iris image database has been used to get the simulation of experiment results which indicate that proposed method increases the compatibility of the iris encryption and also enhance both encryption and decryption phases.

In [49], authors propose a different way to steganalysis of images which are based on CNN. In this technique hierarchical representations can be learnt straight from a pure image, recap and optimize these steps completely. Used CNN structure is completely different from traditional image processing tasks. Instead of a random strategy, CNN's first layer weights are tuned with the main high-pass filter set used in approximation of remaining maps in spartial rich model that works as an organizer to restrain image content efficiency. Truncated linear unit which is a new activation function s used in the model to get the structure of embedding signals. Finally HILL, S-UNIWARD and WOW steganographic algorithms are used to interpret impact of our used model.

In [50], a hyper chaotic image is encrypted by an automatic deep feature extractor which has ability to make preprocessing and fine-tuning. There are many face image databases used to test this algorithm and the results of the method which is proposed by authors show that the algorithm have a better performance according to the traditional deep learning methods. NNs based encryption methods have an increasing trend in the image encryption.

3.3. Advanced Encryption Standard (AES) Based Methods

AES which is invented in 1997 by NIST is an advanced version of Data Encryption Standard (DES). After a comprehensive analysis about mathematical soundness, high encryption speed, high security, defence against most used attack types, free use copyright and because of its eligibility covering a wide range of software and hardware, Rijndael is selected as the algorithm for AES [51]. AES based papers are given in this section.

The researchers in [52] proposed a new reversible data hiding method for encrypted images. Some pixels of image are estimated before encoding in place of hiding data in encoded images straight in order to hide extra data in the estimating errors. An AES based comparative encryption algorithm is implemented to estimate error and the resiude pixels of the image a particular encryption method is designed. No one can access to the original image except those have encryption key. On the other hand, without information about the original image using only data hiding key, extra data can be embedded or extracted. Furthermore, there is not any error for all images during image recovery and the data extraction. Results of this particular experiment indicate that the yield and applicability of the presented technique, particularly in terms of embedded rate versus Peak Signal-to-Noise Ratio (PSNR).

In [53], a combination of cryptography and steganography technique was proposed to overcome the problem of unaccredited information or data access. It is possible to implement steganography to cryptography to rise the security level of data. Proposed technique has three phases which are mosaic image creation, encryption and decryption used by a secret key and finally get the secret image recovery.

3.4. Pixel Value Based Methods

Pixel value techniques are generally used in cover images at steganography. It is based on differences of neighbor pixel values. Some pixel value based researches have been presented briefly in the following. In the proposed method in [54] the cover images that hide the secret image is divided in to three color planes of blue, red and green. Each pixel includes 24-bits which consists of 8 bit components in each pixel. Secret data is embedded in all three components. As a first step, all of the colored pixel is aparted in to three m*n matrix one by one. Pixel Value Modification (PVM) is applied to each plane in order for data hiding. The implanting process of bits have a manner which consist of three steps, each color component of three color spaces are embedded its own matrix. For instance first pixel of red then first pixel of green and at the end first pixel of blue. To enhancement security level, volume and quality of visual more embedding of different numbers of bits applies.

Authors have proposed an image encryption scheme in [55] which is learnable. The basic idea of the proposed scheme is that the network can be trained by using encrypted images, during this process human cannot access images. In this scheme, the network can be trained without obstacles. Cifar dataset is used to confirm the algorithm.

In [56], an algorithm has proposed that makes some improvements to the area of cryptography by using pixel displacement. This algorithm produces cipher images and also decrypt the ciphered image. After all, algorithm uses RGB pixels during this encryption and decryption process.

A high-accuracy scheme which hides digital images is proposed in [57]. This scheme uses a new estimation technique Prediction-Error-Expansion (PEE) and Pixel-Value-Ordering (PVO) techniques. Initially, the main image is divided into blocks which have same sizes. Then according to the pixel values of the each block the minimum and the maximum values of the block are estimated by the rest of pixels. Via PEE data embedding is applied with PVO-based predictor. The combination of PEE and PVO create a benefit in decreasing modified pixels number and so it can avoid lost in image quality. As a result, the method can embed enough data into cover image with minimum distortion. Moreover, provided solution increases the embedding performance according to priory to embed data by using flat blocks. The results show that proposed method have better performance against older techniques.

Pixel Difference Histogram (PDH) analysis can easily be determined by traditional Pixel Value Differencing (PVD) steganographical methods. This problem can be solved by applying two ways

i. using diagonal, vertical and horizontal edges and

ii. make use of adaptive quantization ranges.

An adaptive PVD technique is offered in [58] which uses 6-pixel blocks. The presented adaptive PVD can be applied in two versions, first one is 2x3 pixel-blocks and the second one is 3x2 pixel-blocks. To assign diagonal and horizontal edges, corner pixel values are used to embed data bits. Middle column pixels are used during this process. This is done for all blocks in version 1, likewise same process is done for version 2. This technique has much more hiding capacity and smaller deformity according to common adaptive PVD techniques. Additionally, two different steganalysis which are PDH and Regular/Singular (RS) is not capable to detect this method.

3.5. Least Significant Bit (LSB) Based Methods

LSB based methods are easiest ways in which secret message bits are placed in least significant bits of cover image. Since the word "cover image" is used it means that it is a steganography related technique. In this part, some LSB based researches have been explained.

In [59], authors presented a steganographic technique based on an advanced LSB method for a colored image which is 24-bit and hides an image in itself and cannot be figured out by others. Moreover, this study proves that LSB method for a 24-bit colored image is better than 8-bit colored image. At the beginning, 8-bit and 24-bit LSB methods both are defined after that they are compared by their PSNR, Mean Squared Error (MSE) and histogram values. Algorithm embeds Most Significant Bit (MSB) of the hidden image into LSB of the cover image. By using this this method 6 bits of hidden image can be hide in 24-bit colored image. Finally results show that stego-image cannot be understood by anyone from the original cover image in the case of 24-bit.

A kind of steganography -quantum steganography- is used in [60]. This technique hides data into quantum covers. Two blind LSB steganography algorithms are used. These algorithms are designed as a quantum circuit based on Novel Enhanced Quantum Representation (NEQR). This circuit uses quantum images as secret data. First algorithm is straight LSB that uses the secret message bits to hide in the cover image. Second one is a block LSB that is capable of hiding secret data bit into pixels which are a member of one image block. The secret message can be obtained by using stego images (cover + secret) by the extracting circuits. Experimental results show that hiddenness' of data is good. The stability between capacity and durability can be set with respect to applications.

The study [61] is about image steganography to develop image quality and the security of the image data. The simple LSB algorithm type is used in this study. To develop quality of image that contains secret data which is called stego-image, bit inversion technique is used. Initially, LSB steganography is applied which co-occur with some other bits of image and reduces number of changed LSBs. Then particular LSBs of cover image are reversed. In this way, according to simple LSB method minimum number of least significant bits of cover image is changed so that PSNR of stego-image is developed. Hidden images can be achieved with more accuracy by storing the bit patterns that LSBs are reversed. RC4 algorithm has been applied to succeed the randomization instead of sequent order of hidden image bits into cover image pixels. In this way, hidden message bits are distributed randomly to the cover image.

In [62], authors have designed a mobile application which uses AES and LSB respectively to encrypt images and to hide encrypted image to another image. 256-bit length key of AES is used for high level security. For protection of key, Diffie-Hellman algorithm is used against unauthorized access. In this study as the project development methodology, Rapid Application Development (RAD) model is used. It let the phase to iterate until the application is developed. By the way needs are collected and let the early testing of the prototypes throughout each iteration to reduce the any big problems in the final distribution of the application. Application is interpreted by using ISO/IEC/IEEE 29119 Testing Standards. In this evaluation, reliability, security and usability of the application were handled. As a result, good performance rating is obtained.

The study [63] uses cryptography and steganography to make transmission secure and confidential. Actually modification of Vigenere Cipher, LSB and Dictionary Based Compression (DBC) methods realize this processes. PSNR is used to determine the performance of the study, at the same time Spread Spectrum and Pixel Value Differencing methods are compared with this study in terms of performance. As a result of comparison this study has a better performance according to the aforementioned methods.

3.6. Exclusive OR (XOR) Based Methods

XOR (Exclusive OR) is a logical operation such as OR, AND and NOT. This method provides a robustness in security. Many different variations of the use of XOR exist at the image processing area. Some of these variations are mentioned below.

In [64], encryption and decryption stages include some steps; original image is assumed as a matrix and then this matrix is divided into blocks, each blocks have equal sizes which is 8 bytes. After that a few secret key are specified. Key sizes must be equal to block sizes and in the range of 0-255. Decryption stage starts with getting the encrypted colored image matrix. The obtained image is in 3D. Final image is reshaped into 1D. Obtained image matrix is divided into 8-byte equal block sizes. 4 private keys are used with elements; each key is used with 8 elements. Each data block is exposed to XOR with key4, key3, key2, and key1 one by one. Finally, decrypted blocks are obtained, to get the decrypted image this blocks must be reshaped.

The study [65] includes to stage steganography and cryptography, for the first stage sequential algorithm is used and for the second stage symmetric XOR is used. In [66], a secret message is embedded in to a colored cover image. Initially, the starting position in the cover image and the length of the message is defined. The starting position of the message can be accepted as key1 which is first secret private key. After that one byte of the image is reserved to one character of the message this is the insertion stage. Colored image is reshaped from 3D matrix to 2D matrix. These resulting matrices are divided into equal size blocks (4x4). Key2 as a secret private key is selected which has 4x4 size and in the range 0-255. Then XOR is applied to each block with key2 to get encrypted 2D matrix. After that encrypted color image and key2 are saved. Colored image decryption also have some steps, initially 3D image is reshaped to 2D matrix. Then image is divided into 4x4 blocks and XOR is applied to each block with key2 to obtain 2D decrypted image matrix. 2D decrypted image matrix is converted to 3D to get the decrypted colored image. Finally, to get the secret message by using key1 we extract the characters of the message.

3.7. Discrete Cosine Transform (DCT) Based Methods

DCT is an image compression technique. It is useful where a large amount of image need to be stored. Images are separated into parts of several frequencies this process is called quantization. In this process frequencies are separated as most important and less important. During retrieval process the less important frequencies are discarded only the most important frequencies are used. This is how DCT runs. In this part some DCT based studies are handled.

In [67], a new steganography technique which is deformity function for images is proposed. This technique is based on quantity of zeros in a DCT block, residual of the first and second-order and magnitude of the DCT coefficients.

The capability of prevailing coefficient to hide alteration trace is depending on the magnitude of a DCT coefficient. Residual of the consecutive orders which is first and second make enough use of the correlation in DCT domain, this order residuals make sufficient utilization of correlation in DCT domain, and the block texture is well if the amount of zeros in a DCT block are enough. The combination of these parameters is used to calculate the detection risks because of change in the cover data. In this way the changes which are done by humans are not detectable in the stego-image.

In [68], authors proposed a technique which uses consecutive zero coefficients in zigzag sequences of DCT blocks for images. This technique can also be called as adaptive real-time reversible data hiding.

This proposed scheme keeps the quality of stego-image and reversibility while increases the hiding capacity. Experimental results of this scheme shows that it increases the performance, image quality also keeps data hiding capacity.

A steganography method which presents a noval channel selection rule is proposed in [69]. This method can be used to find DCT coefficients that may present minimal discoverable defect to hide data. For the proposed channel selection rule three elements are planned. These elements are the Quantization Step (QS), the Perturbation Error (PE) and the size of DCT quantized coefficient that are to be modified (MQ). Results of the experiments show that by using this noval channel selection rule better security performance can be achieved.

In [70], a new method to encrypt and decrypt of an RGB image have been proposed by using two stage random matrix affine cipher which is incorporated with discrete wavelet transformation. Previous studies about encryption and decryption of images debated just about the keys, however in this method arrangement of Random Matrix Affine Cipher (RMAC) parameters and keys are essential. To encode and decode an RGB image, a formula is prepared which choose keys for all possible range. Capability of proposed method has analyzed by a simulation. Results show that this method can be used effectively for image data and also it is secure.

3.8. Reversible Data Hiding Based Methods

Reversible data hiding is a technique which hides secret message data into cover image or video. Then on the receiver side the secret data is extracted and rebuilt by using a reversible method. In this part some different studies are briefly discussed which are use reversible data hiding.

In [71] to preserve data embedding and image privacy a Reversible Data Hiding in Encrypted Images (RDHEI) has been proposed. The method includes three parts: first part is image provider, second part is data hider and the final part receiver. There are three types of key regulation for security these are Share No Secret Keys (SNK), Independent Secret Keys (SIK) and Shared One Key (SOK). In SNK secret key is never shared but in SIK image provider and data hider parts have to share secret key with the receiver part orderly. In many studies SNK-type schemes are proposed which use homomorphic encryption. In this study SOK setting is addressed, where secret key is shared with the receiver by the image provider, and a secret data can be hided into image by data hider. During this embed process there is no information about the key. Actually a multi-secret sharing technique is used as the basic encryption, which causes explosion of the key size. To avoid such key size problem a compression algorithm is applied which is a lightweight cryptographic technique.

In [72], a new reversible scheme is proposed which works on encrypted images. Actual image is encoded by using encryption key to provide confidentiality. After that by using one secret bit all of particular block of the encoded image is embedded. This processes are performed by data hider by using data-hiding key. Owing to detailed selection for fractional pixels to be flipped, small changes to each block is directed by data hiding operation that guide important improvement of decrypted image quality. By using the marked, encryption key and encoded data can be decoded and then through the data-hiding key the hidden data of the decrypted image is extracted.

Reversible data hiding techniques generally makes some changes on the cover image. In this way there may occur some unavoidable traces of this changes so those who wants to catch the data can simply attack. In [73], a new Generative Reversible Data Hiding (GRDH) scheme is proposed which is originate from cover synthesis steganography-based Generative Adversarial Networks (GANs). By using CycleGAN model which is image-to-image translation model a realist image is generated. Then a stego-image (cover image with the secret image) that has dissimilar semantic information will be produced. After transmission by using the inverse transformation and trained message extractor, the stego-image can easily be recovered. Experimental results show the efficiency of the proposed technique.

In [74], a reversible cellular automata image encode method is proposed to obtain similar search on encoded domain. For the personal information privacy some important images like private images and medical images have to be encoded during transmission, which make content-based image recapture technic on plaintext domain pointless. In this technique, as a first step similarity search is defined on encoded images and applicability of pixel-based deterministic encryption is analyzed and a Deterministic Encryption Based on Reversible Cellular Automata (DERCA) is offered. Then to extract colored image histogram from encrypted image, a multi-level-granularity image encryption is offered, which is based on DERCA. To overcome from utility-security quandary pixels of image are encrypted in pixel-set-granularity or pixel-granularity. To increase image security and retrieval correctness, block-based permutation technique is applied.

In [75], a new reversible scheme to data hiding is proposed. Initially, by using a stream cipher, the whole data of which is not compressed image is encoded, and the extra data is embedded into the image by changing a small part of encoded data. Primarily an encoded image which include extra data is decoded via encryption key, and a decrypted image is obtained which is like to original image. With the help of spatial correlation of natural image, the hided data can perfectly have original image and extracted part.

3.9. Genetic Algorithm (GA) Based Methods

GA based cryptography is a new method used in cryptography area. According to traditional cryptographic methods it has an efficient security and fast growing bio molecular computation ability. There are some GA based papers below.

Key selection is very important in public key cryptography. Keys are classified according their fitness function and to make GA a good choice for the key generation. In [18], authors propose a technique of GA for encryption and decryption of the data.

In [19], a DNA-Genetic Encryption Technique (D-GET) is proposed to obtain a stronger technique in terms of secure. In this method binary form of the any type of digital data is converted to DNA sequences then respectively reshape, encrypt, crossover, mutate and then reshape, steps are applying. D-GET stages are repeated minimum three times. Data is transmitted in text or image format file. On the other hand, D-GET is used to decrypt the accepted data and reshape it to original format by the receiver. Transformation of the textual data into an image is possible and also the opposite of this is also possible in this technique.

By doing this, security is improved. Increasing in degree of diffusion and confusion is done by multiple key sequences. Cipher data has a perfect security so it is very difficult to decipher. According to experimental results the proposed technique has a multilayer protection stages across various attacks.

Medical images are very important in diagnosis of illnesses so to avoid unauthorized accesses over the network, these images must be encrypted. The study [76] is based on a hybrid model of coupled map lattices and the Modified Genetic Algorithm (MGA). This technique initially uses coupled map lattice to produce the amount of secure encrypted images to primary population of MGA. Secondly the proposed method implements MGA to reduce the algorithm computational time and to increment the entropy of the encrypted images.

3.10. Combined Methods

There are many image encryption methods to make transmission and data store secure. Generally, a single method is used during encryption and decryption processes. But sometimes multiple methods combined to obtain a better security and to make unauthorized access almost impossible to data which are transmitted or stored. The table below shows the combined methods which are discussed in this paper.

***Table 1.** Combined Methods with their advantages*

Reference	Combined Methods	Advantages
[77]	DES, AES and Blowfish	-AES provides encryption / decryption speed and security
[78]	GLM and MLE	-Improved quality of stego-images, high imperceptibility -Cost effectiveness -Enhanced robustness
[79]	Chaos and NNs	-Guaranteed high secured
[80]	Chaos and NNs	-Robust against various cryptanalysis (plaintext-only and chosen-plaintext attacks)
[81]	Crossover Operator, Chaos and SHA-2	-Good encryption (through only one round encryption process)
[82]	DNA and Chaos	-Increase the algorithm complexity -Cipher text unpredictability
[83]	Cryptography with probabilistic and Homomorphic properties	-Lossless and combined information hiding plans
[84]	Generalized Arnold Transform and Double Random-Phase Encoding	-Very large key space -Validity and the reliability -Lower computational complexity
[85]	XOR and Bits shuffling	-Multiple barriers in the way of an attacker
[86]	Chaos and Bit Operations	-Effective image encryption
[87]	DNA and Chaos	-Satisfactory encryption effect on security -Robustness
[88]	LSB and Hill Cipher	-Secure data
[89]	LSB and XOR	-Overcomes the limitation of the existing methods (The data hiding capacity is 100% as all the pixel can carry data bit)
[90]	T-DES and LSB	-Good quality of stego-image
[91]	AES and LSB	-Higher level of security
[93]	Chaos and XOR	-Encryption of color, gray and binary images in an efficient way with higher security -Limited resource utilization
[95]	LPT and DRPE	-Flexible in encrypting multiple images
[96]	Cost Based Algorithms (HUGO, S-UNIWARD, and HILL)	-Better security (owing to parallel images)
[97]	Spread Spectrum Method and Cryptography	-Very high level of security

[98]	Palette and Minimum Spanning Tree	-Improvement in security -Camouflage of the stego-image
[99]	Chaotic Systems and Elliptic Curve El-Gamal Scheme	-Dual layer of security -Large key space of the encryption scheme to resist brute-force attacks

where GLM is Gray Level Modification, MLE is Multi-Level Encryption, SHA is Secure Hash Algorithm, LPT is Log-Polar Transform and DRPE is Double Random Phase Encoding.

Some combined methods have disadvantages besides their advantages. The combined method used in [92] which consist of Hill Cipher and Cryptography techniques is unusable for any security sensitive application. The method in [94] which is a combination techniques of Markovian and NNs needs to much time for encryption and decryption.

3.11. Specific Methods

Except the most known image encryption methods dozens of specific ones also exist. Some of these methods are reputed in the other computer science areas but they adapted to image encryption field.

In [100], authors have built three important basic classification protocols which fullfit privacy limitations: Naïve Bayes, decision trees, and hyperplane decision. The main principle of these structures is to build a set of privacy-preserving classifiers. It is proven that how to these structures can be used to build other classifiers than aforesaid structures, like a face detection classifier and multiplexer. According to test results the performance of these structures are efficient when real medical datasets are used.

In [101], a new method based on Huffman Encoding, is proposed for image steganography. Two images are used as secret image and cover image. Both of these images are 8-bit gray level image and their sizes are e*f and t*q. Before embedding secret image Huffman Encoding is applied. After that every particular bit of Huffman code of secret message is hided into the cover image by changing the LSB of pixel's intensities of cover image. Some other data also embedded into cover image such as Huffman Table and size of the Huffman encoded bit stream therefore the stego-image becomes an independent data to the receiver. Results of this experiment shows that this method is too secure since Huffman table and decoding rules are not known.

Study in [102] proposed a 64-bits Blowfish which is a secret key block cipher to provide an advance performance and security. The key size of this algorithm can be vary up to 448-bits. Feistel network is used that repeat simple function 16 times. The Blowfish algorithm has a fast process ability according to known popular algorithm and protect from unauthorized accesses. For this experiment MATLAB has been used. Some other specific methods have been listed in the table below.

Table 2. *Specific methods*

Reference	Methods
[103]	Brownian Motion
[104]	DHTTIE
[105]	Parallel Diffusion Method
[106]	Finite Field Cosine Transform
[107]	Binary Bitplane
[108]	Elliptic Curve Cryptography
[109]	Visual Cryptograms of Random Grids
[110]	Adaptive Encoding Algorithm

[111]	RC4 Algorithm
[112]	Reserving Room Before Encryption with a Traditional RDH Algorithm
[113]	Byte Manupilation
[114]	Fourier Transform
[115]	Fresnel and Fractional Fourier Transform Domains
[116]	Hash Codes
[117]	RSA
[118]	Hill Cipher
[119]	IWT
[120]	Haar Wavelet Transform
[121]	Canny Edge Detection Algorithm
[122]	Quantum Image Geometric Transformations
[123]	SSP
[124]	Steganography
[125]	Cryptography
[126]	Random Embedding Method
[127]	Patch-Level Sparse Representation
[128]	Cover-Source Switching
[129]	One-Time Pad Encryption
[130]	Universal Distortion Function
[131]	Homomorphic Cryptographic Solutions

where DHTTIE is Diffie Hellman Text-to-Image Encryption Algorithm, IWT is Integer Wavelet Transform, SSP is Secure Simple Pairing, RDH is Reversible Data Hiding.

4. RESULTS AND DISCUSSION

In this study, the handled papers have been compared with each other by various specifications which are used image name, type, format, count, size, publication year of the papers and so on. Many statistical outcomes obtained and then presented graphically.There are some very known images in image processing researches such as Lena, Baboon, Pepper, Barbara, Cameraman, Tiffany, Airplane, Sailboat and Haouse. It is not an obligation to use this popular images in the studies and some authors use their specific images during their research but when these images are used, it is easy to make comparisons.

As it is seen in Figure 1. most of the researchers have used basic image processing photos. Secondly, authors have used unknown (in image processing field) images that are their own preference. As a third option some datasets (MNIST, CIFAR-10, AT&T, FaceScrub and so on) have been used by authors to perform their research.

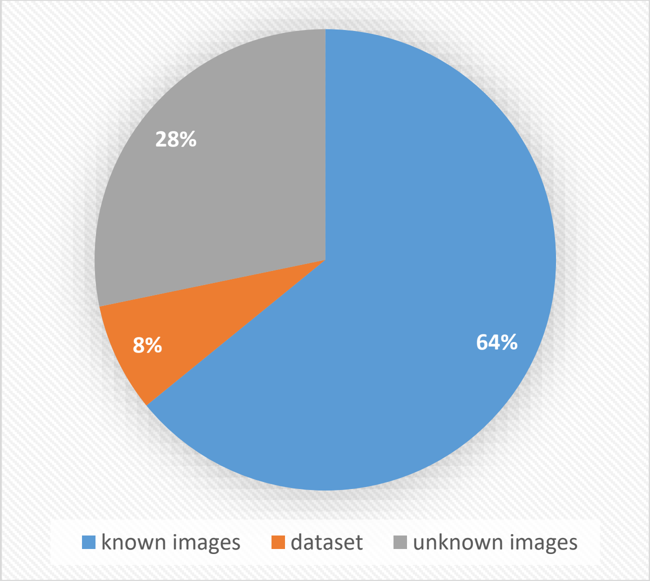

Figure 1. *Percentage of the used images that are familiar or not at image processing area.*

In Fig. 2. percentages of used images in handled papers is shown. Lena has the highest usage percentage which is the most famous image. Baboon and Pepper are enough known images too. Then the other popular images come after each other. These images are shown in Figure 3. below.

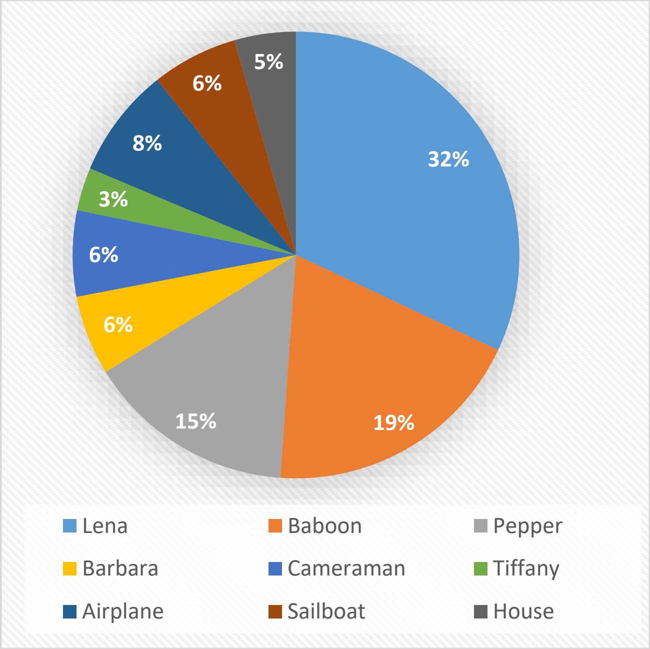

Figure 2. *Percentage of the known image that are used.*

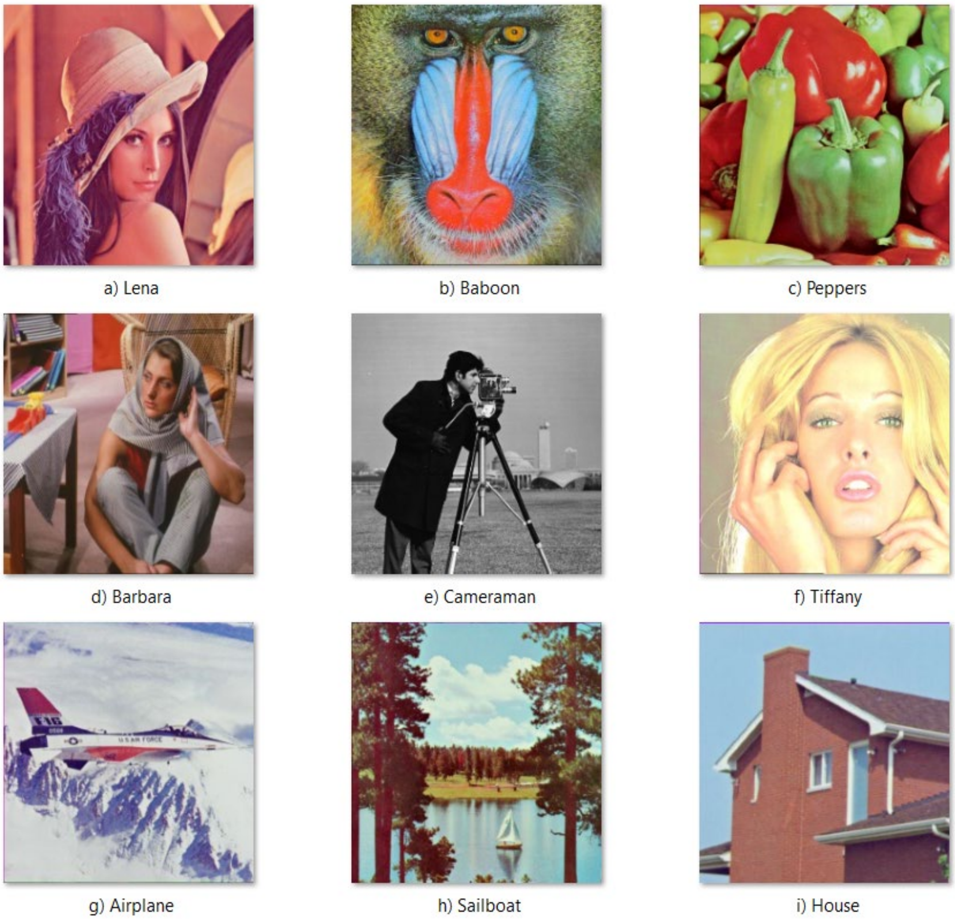
a) Lena
b) Baboon
c) Peppers
d) Barbara
e) Cameraman
f) Tiffany
g) Airplane
h) Sailboat
i) House

Figure 3. *Popular images.*

In some studies, just one of these images has been used, while in others more than one of these images have been used. There are also studies in which all these images are used together. By the way in some researches it has not specified whether it is single image or multi-image is used. Figure 4. shows this information graphically.

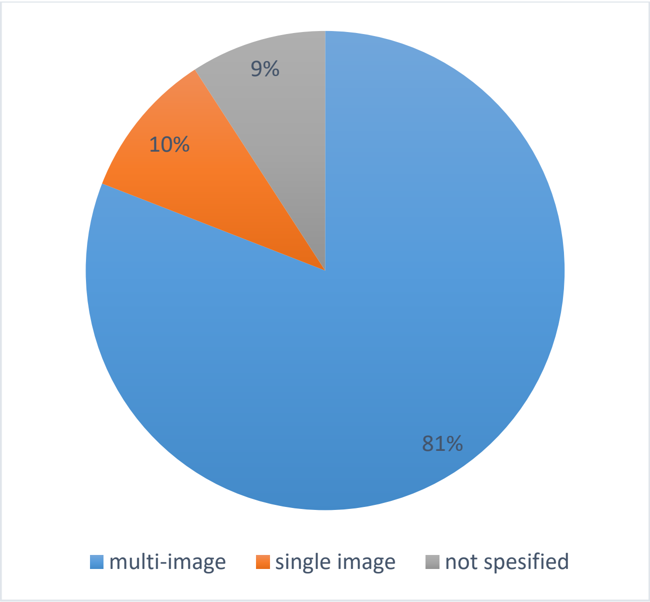

Figure 4. *Percentage of the quantitative of images used in each paper.*

Figure 5. implements percentage of used images that are gray scale or colored. In handled papers mostly gray scale images have been used, colored images usage is less than grayscale images. 15% of studies have used both colored and grayscale images together. The difference between colored images and gray scale images is that grayscale images pixels have just one dimension where colored images have 3 dimensions RGB. In a grayscale image each particular pixel has intensity value between 0-255. In a colored image, each pixel has three values between 0-255.

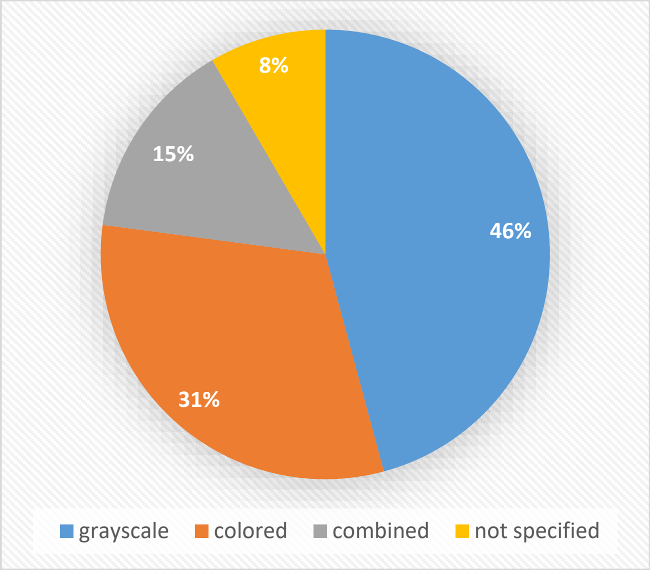

Figure 5. *Percentage of the image that are whether colorful or not.*

There are many image formats such as jpeg, bmp, png, tiff and gif and they have different characteristics. As a comparison, when a jpeg image decreases in file size also quality of image decreases in the other side a png image is "lossless" this means it can be edit and no lose in quality but this does not change the fact that png images have low resolution. In Figure 6. usage percentage of image formats is given. Great majority of authors have not specified the format of used image in their research. 8% of them have used more than one format and a small part of them have used BMP and JPEG formats respectively.

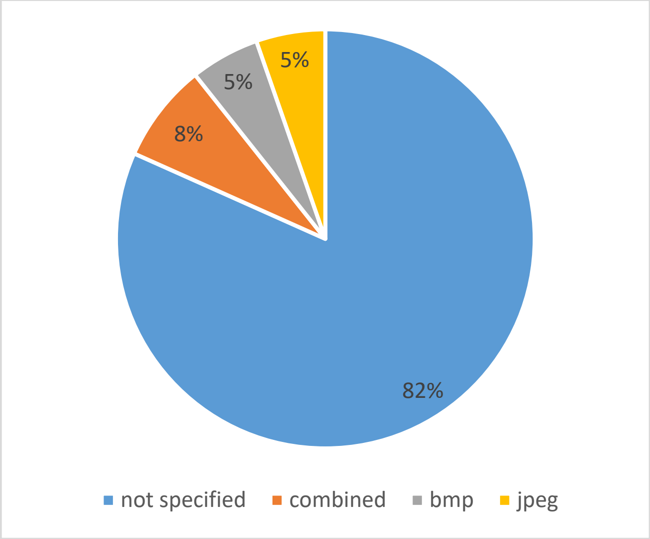

Figure 6. *Percentage of the image formats.*

There are some specific and most used image sizes that give us a square view such as 64x64, 128x128, 256x256, 512x512, 1024x1024. It is not an obligation to use this specific sizes in researches it is up to author(s). In Figure 7. sizes of images that are used in handled studies are shown. 11% of authors have used different sizes that they specify.

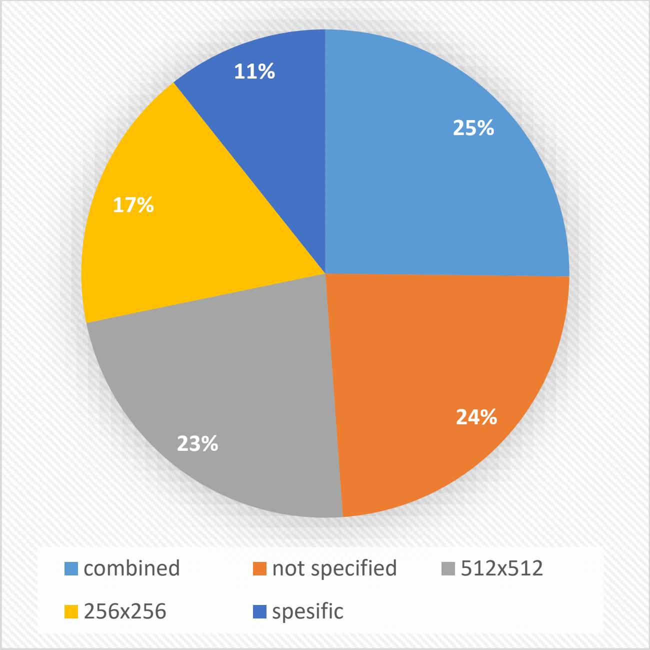

Figure 7. *Percentage of the image sizes.*

Figure 8. shows the changes in number of papers in terms of years. As image encryption has become popular in recent years, the number of articles in this area has been increasing generally year by year. In handled articles the year 2018 has the biggest share. Since the developments in this area have an increasing trend the number of articles also will ascend.

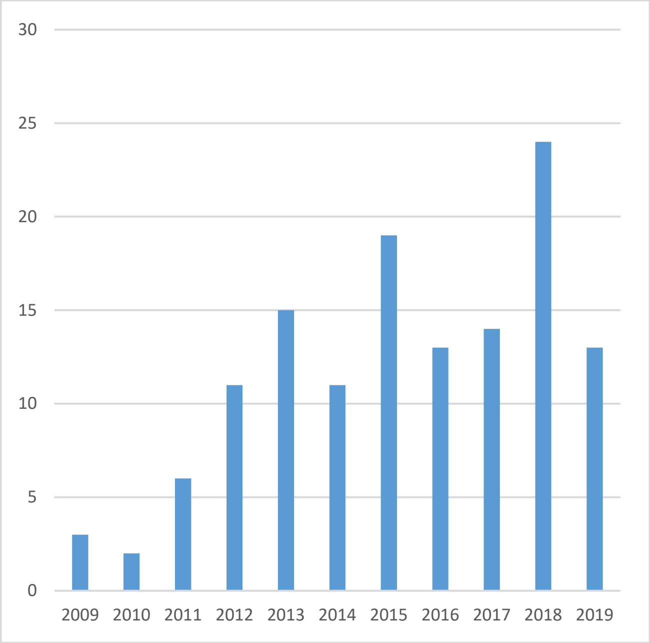

Figure 8. *Distribution of the papers according to the years.*

5. CONCLUSION

Nowadays, technology is advancing very rapidly and in this context, the fields of study affected by technological developments have to update themselves according to the developing technology in order to ensure their continuity. Images are an important data type used in many fields. In this case, necessary and sufficient security precautions must be taken for both the storage of images and the transfer of images over the network, otherwise malicious individuals or entities may capture the images with new methods they develop. Thanks to the developing technology, new methods have been added to traditional methods that provide data security or methods used in different fields have begun to be used effectively in providing data security.

In this study, encryption methods and approaches used in both colored and gray level images are examined and classified according to the method on which it is based. While several traditional methods were used together in some articles, in other studies either completely newly developed techniques were used or new methods were used in combination with traditional methods.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest regarding the publication of the paper.

REFERENCES

[1] C. K. Volos, I. M. Kyprianidis and I. N. Stouboulos, Image encryption process based on chaotic synchronization phenomena. Signal Processing, 93:5 (2013) 1328-1340.

[2] A. Kanso and M. Ghebleh, An algorithm for encryption of secret images into meaningful images. Opt. Lasers Eng., 90:2016 (2017) 196–208.

[3] G. Srividya and P. Nandakumar, A Triple-Key chaotic image encryption method. ICCSP 2011–Int. Conf. Commun. Signal Process., (2011) 266–270.

[4] A. V. Diaconu and K. Loukhaoukha, An improved secure image encryption algorithm based on rubik's cube principle and digital chaotic cipher. Math. Probl. Eng., 2013:1 (2013).

[5] X. Wu, Y. Li and J. Kurths, A new color image encryption scheme using CML and a fractional-order chaotic system. PLoS One, 10:3 (2015) 1–28.

[6] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho and S. W. Baik, Image steganography using uncorrelated color space and its application for security of visual contents in online social networks. Futur. Gener. Comput. Syst., 86 (2018) 951–960.

[7] M.Khan, A. Jamil, F. Haleem, Z. Muhammad, A Novel Image Steganographic Approach for Hiding Text in Color Images using HSI Color Model. Middle-East Journal of Scientific Research, 22 (2014) 647-654.

[8] A. M. Shaheen, T. R. Sheltami, T. M. Al-Kharoubi and E. Shakshuki, Digital image encryption techniques for wireless sensor networks using image transformation methods: DCT and DWT. J. Ambient Intell. Humaniz. Comput., 10:12 (2019) 4733–4750.

[9] H. R. Kanan and B. Nazeri, A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm. Expert Syst. Appl., 41:14 (2014) 6123–6130.

[10] K. Shankar, M. Elhoseny, R. S. Kumar, S. K. Lakshmanaprabu and X. Yuan, Secret image sharing scheme with encrypted shadow images using optimal homomorphic encryption technique. J. Ambient Intell. Humaniz. Comput., 11:5 (2020) 1821–1833.

[11] S. Bukhari, M. S. Arif, M. R. Anjum and S. Dilbar, Enhancing security of images by Steganography and Cryptography techniques. INTECH 2016–6th Int. Conf. Innov. Comput. Technol., (2017) 531–534.

[12] G. Ye, C. Pan, X. Huang and Q. Mei, An efficient pixel-level chaotic image encryption algorithm. Nonlinear Dyn., 94:1 (2018) 745–756.

[13] H. Kaur and A. Kakkar, Comparison of different image formats using LSB Steganography. ISPCC 2017 - 4th IEEE Int. Conf. Signal Process. Comput. Control, (2017) 97–101.

[14] F. Han, X. Liao, B. Yang and Y. Zhang, A hybrid scheme for self-adaptive double color-image encryption. Multimed. Tools Appl., 77:11 (2018) 14285–14304.

[15] Y. Zhang, Y. Li and J. Su, Iterative learning control for image feature extraction with multiple-image blends. Eurasip J. Image Video Process., 2018:1 (2018) 1–11.

[16] D. R. I. M. Setiadi, E. H. Rachmawanto and C. A. Sari, Secure Image Steganography Algorithm Based on DCT with OTP Encryption. J. Appl. Intell. Syst., 2:1 (2017) 1–11.

[17] V. Thakur and M. Saikia, “Hiding secret image in video, ISSP 2013 - Int. Conf. Intell. Syst. Signal Process., (2013) 150–153.

[18] R. Jhingran, V. Thada and S. Dhaka, A Study on Cryptography using Genetic Algorithm. Int. J. Comput. Appl., 118:20 (2015) 10–14.

[19] H. M. Mousa, DNA-Genetic Encryption Technique. Int. J. Comput. Netw. Inf. Secur., 8:7 (2016) 1–9.

[20] M. A. F. Al-Husainy, A novel encryption method for image security. Int. J. Secur. its Appl., 6:1 (2012) 1–8.

[21] P. Li, C. N. Yang and Q. Kong, A novel two-in-one image secret sharing scheme based on perfect black visual cryptography. J. Real-Time Image Process., 14:1(2018) 41–50.

[22] J. Chao et al., CaRENets: Compact and Resource-Efficient CNN for Homomorphic Inference on Encrypted Medical Images. Arxiv abs, (2019).

[23] R. McPherson, R. Shokri and V. Shmatikov, Defeating Image Obfuscation with Deep Learning. Corr abs, (2016).

[24] K. K. S. Pareek, K. Narendra K and V. Patidar, A Symmetric Encryption Scheme for Colour BMP Images. IJCA Spec. Issue Network Secur. Cryptogr., 2014 (2011) 42-46.

[25] X. J. Tong, M. Zhang, Z. Wang, Y. Liu, H. Xu and J. Ma, A fast encryption algorithm of color image based on four-dimensional chaotic system. J. Vis. Commun. Image Represent., 33 (2015) 219–234.

[26] H. I. Hsiao and J. Lee, Color image encryption using chaotic nonlinear adaptive filter. Signal Processing, 117 (2015) 281–309.

[27] Y. Zhou, L. Bao and C. L. P. Chen, A new 1D chaotic system for image encryption. Signal Processing, 97 (2014) 172–182.

[28] S. S. Askar, A. A. Karawia, A. Al-Khedhairi and F. S. Al-Ammar, An algorithm of image encryption using logistic and two-dimensional chaotic economic maps. Entropy, 21:1 (2019) 1–17.

[29] C. Zhu, A novel image encryption scheme based on improved hyperchaotic sequences. Opt. Commun., 285:1 (2012) 29–37.

[30] N. Bigdeli, Y. Farid and K. Afshar, A robust hybrid method for image encryption based on Hopfield neural network. Comput. Electr. Eng., 38:2 (2012) 356–369.

[31] L. Wang, H. Song and P. Liu, A novel hybrid color image encryption algorithm using two complex chaotic systems. Opt. Lasers Eng., 77 (2016) 118–125.

[32] S. S. Askar, A. A. Karawia, and A. Alshamrani, Image encryption algorithm based on chaotic economic model. Math. Probl. Eng., 2015 (2015).

[33] T. Kumar and S. Chauhan, Image Cryptography with Matrix Array Symmetric Key using Chaos based Approach. Int. J. Comput. Netw. Inf. Secur., 10:3 (2018) 60–66.

[34] Y. Abanda and A. Tiedeu, Image encryption by chaos mixing. IET Image Process., 10:10 (2016) 742–750.

[35] R. Roy, A. Sarkar and S. Changder, Chaos based Edge Adaptive Image Steganography. Procedia Technol., 10 (2013) 138–146.

[36] X. Wang, L. Teng, and X. Qin, A novel colour image encryption algorithm based on chaos. Signal Processing, 92:4 (2012) 1101–1108.

[37] Z. Wang, F. Min, and E. Wang, A new hyperchaotic circuit with two memristors and its application in image encryption. AIP Adv., 6:9 (2016).

[38] M. A. Hussain and P. Bora, A Highly Secure Digital Image Steganography Technique Using Chaotic Logistic Map and Support Image. ICICSP 2018–IEEE Int. Conf. Inf. Commun. Signal Process. no. Icsp, (2018) 69–73.

[39] R. Rhouma, S. Meherzi and S. Belghith, OCML-based colour image encryption. Chaos, Solitons and Fractals, 40:1 (2009) 309–318.

[40] X. Wang and D. Zhao, Fully phase multiple-image encryption based on superposition principle and the digital holographic technique. Opt. Commun., 285:21 (2012) 4280–4284.

[41] S. Dogan, A New Approach for Data Hiding based on Pixel Pairs and Chaotic Map. Int. J. Comput. Netw. Inf. Secur., 10:1 (2018) 1–9.

[42] Y. Luo, M. Du and J. Liu, A symmetrical image encryption scheme in wavelet and time domain. Commun. Nonlinear Sci. Numer. Simul., 20:2 (2015) 447–460.

[43] M. A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, R. M. López-Gutiérrez and O. R. Acosta Del Campo, A RGB image encryption algorithm based on total plain image characteristics and chaos. Signal Processing, 109 (2015) 119–131.

[44] B. Isac and V. Santhi, A Study on Digital Image and Video Watermarking Schemes using Neural Networks. Int. J. Comput. Appl., 12:9 (2011) 1–6.

[45] E. Hesamifard, H. Takabi and M. Ghasemi, CryptoDL: Deep Neural Networks over Encrypted Data. Arxiv abs., (2017) 1–21.

[46] P. Xie, M. Bilenko, T. Finley, R. Gilad-Bachrach, K. Lauter and M. Naehrig, “Crypto-Nets: Neural Networks over Encrypted Data. Arxiv abs., (2014) 1–9.

[47] A. A. Zaidan, B. B. Zaidan, Y. A. Taqa, M. K. Sami, G. M. Alam and A. H. Jalab, Novel multi-cover steganography using remote sensing image and general recursion neural cryptosystem. Int. J. Phys. Sci., 5:11 (2010) 1776–1786.

[48] X. Li, Y. Jiang, M. Chen and F. Li, Research on iris image encryption based on deep learning. Eurasip J. Image Video Process., 2018:1 (2018).

[49] J. Ye, J. Ni and Y. Yi, Deep Learning Hierarchical Representations for Image Steganalysis. IEEE Trans. Inf. Forensics Secur., 12:11 (2017) 2545–2557.

[50] Y. Qin, C. Zhang, R. Liang and M. Chen, Research on Face Image Encryption Based on Deep Learning. IOP Conf. Ser. Earth Environ. Sci., 252:5 (2019).

[51] K. R. Saraf, V. P. Jagtap and A. K. Mishra, Text and Image Encryption Decryption Using Advanced Encryption Standard. Int. J. Emerg. Trends Technol. Comput. Sci., 3:3 (2014) 118.

[52] W. Zhang, K. Ma and N. Yu, Reversibility improved data hiding in encrypted images. Signal Processing, 94:1 (2014) 118–127.

[53] M. Joseph, Mosaic Image Steganography Based Colour Transformation for Enhanced Security. IJMTER, 2:10 (2015) 149–156.

[54] V. Nagaraj, V. Vijayalakshmi and G. Zayaraz, Color Image Steganography based on Pixel Value Modification Method Using Modulus Function. IERI Procedia, 4 (2013) 17–24.

[55] M. Tanaka, Learnable Image Encryption. ICCE-TW 2018-IEEE Int. Conf. Consum. Electron., (2018) 1-2.

[56] Q. A. Kester and K. M. Koumadi, Cryptographie technique for image encryption based on the RGB pixel displacement. ICAST 2012–IEEE 4th Int. Conf. Adapt. Sci. Technol., (2012) 74–77.

[57] X. Li, J. Li, B. Li and B. Yang, High-fidelity reversible data hiding scheme based on pixel-value-ordering and prediction-error expansion. Signal Processing, 93:1 (2013) 198–205.

[58] A. Pradhan, K. R. Sekhar and G. Swain, Adaptive PVD steganography using horizontal, vertical, and diagonal edges in six-pixel blocks. Secur. Commun. Networks, (2017).

[59] D. Rawat and V. Bhandari, A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image. Int. J. Comput. Appl., 64:20 (2013) 15–19.

[60] N. Jiang, N. Zhao and L. Wang, LSB Based Quantum Image Steganography Algorithm. Int. J. Theor. Phys., 55:1 (2016) 107–123.

[61] N. Akhtar, P. Johri and S. Khan, Enhancing the security and quality of lsb based image steganography. CICN 2013–5th Int. Conf. Comput. Intell. Commun. Networks, (2013) 385–390.

[62] R. E. Castillo, P. J. M. Castro, G. T. Cayabyab and M. Rachel Aton, Blocksight: A mobile image encryption using advanced encryption standard and least significant bit algorithm. ACM International Conference no. November, (2018) 117–121.

[63] Rojali, A. G. Salman and G. George, Website-based PNG image steganography using the modified Vigenere Cipher, least significant bit, and dictionary based compression methods. AIP Conference, 1867 (2017).

[64] M. O. Al-Dwairi, A. Y. Hendi and Z. A. Alqadi, An Efficient and Highly Secure Technique to Encrypt and Decrypt Color Images. Technol. Appl. Sci. Res., 9:3 (2019) 4165–4168.

[65] M. Saritha, V. M. Khadabadi and M. Sushravya, Image and text steganography with cryptography using MATLAB. Int. Conf. Signal Process. Commun. Power Embed. Syst. SCOPES 2016, (2017) 584–587.

[66] R. Rasras, Z. AlQadi and M. Sara, A Methodology Based on Steganography and Cryptography to Protect Highly Secure Messages. Eng. Technol. Appl. Sci. Res., 9:1 (2019) 3681–3684.

[67] Z. Wang, Z. Yin and X. Zhang, Distortion Function for JPEG Steganography Based on Image Texture and Correlation in DCT Domain. IETE Tech. Rev. (Institution Electron. Telecommun. Eng. India), 35:4 (2018) 351–358.

[68] C. N. Yang, C. Kim and Y. H. Lo, Adaptive real-time reversible data hiding for JPEG images. J. Real-Time Image Process., 14:1 (2018) 147–157.

[69] F. Huang, J. Huang and Y. Q. Shi, New channel selection rule for JPEG steganography. IEEE Trans. Inf. Forensics Secur., 7:4 (2012) 1181–1191.

[70] M. Kumar, D. C. Mishra and R. K. Sharma, A first approach on an RGB image encryption. Opt. Lasers Eng., 52:1 (2014) 27–34.

[71] Y. C. Chen, T. H. Hung, S. H. Hsieh and C. W. Shiu, A New Reversible Data Hiding in Encrypted Image Based on Multi-Secret Sharing and Lightweight Cryptographic Algorithms. IEEE Trans. Inf. Forensics Secur., 14:12 (2019) 3332–3343.

[72] C. Qin and X. Zhang, Effective reversible data hiding in encrypted image with privacy protection for image content. J. Vis. Commun. Image Represent., 31 (2015) 154–164.

[73] Z. Zhang, G. Fu, F. Di, C. Li and J. Liu, Generative Reversible Data Hiding by Image-to-Image Translation via GANs. Secur. Commun. Networks, (2019).

[74] Y. Su, Y. Wo and G. Han, Reversible cellular automata image encryption for similarity search. Signal Process. Image Commun., 72 (2018) 134–147.

[75] X. Zhang, Reversible data hiding in encrypted image. IEEE Signal Process. Lett., 18:4 (2011) 255–258.

[76] H. Nematzadeh, R. Enayatifar, H. Motameni, F. G. Guimarães and V. N. Coelho, Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices. Opt. Lasers Eng., 110 (2018) 24–32.

[77] A. Devi, A. Sharma and A. Rangra, A Review on DES, AES and Blowfish for Image Encryption & Decryption. Int. J. Eng. Comput. Sci., 4:6 (2015) 12646–12651.

[78] K. Muhammad, J. Ahmad, H. Farman, Z. Jan, M. Sajjad and S. W. Baik, A secure method for color image steganography using gray-level modification and multi-level encryption. KSII Trans. Internet Inf. Syst., 9:5 (2015) 1938–1962.

[79] S. B. Suryawanshi and D. D. Nawgaje, a Triple-Key Chaotic Neural Network for Cryptography in Image Processing. Int. J. Eng. Sci. Emerg. Technol., 2:1 (2012) 2231–6604.

[80] K. Ratnavelu, M. Kalpana, P. Balasubramaniam, K. Wong and P. Raveendran, Image encryption method based on chaotic fuzzy cellular neural networks. Signal Processing, 140 (2017) 87–96.

[81] R. Guesmi, M. A. Ben Farah, A. Kachouri and M. Samet, Hash key-based image encryption using crossover operator and chaos. Multimed. Tools Appl., 75:8 (2016) 4753–4769.

[82] Q. Zhang, L. Liu and X. Wei, Improved algorithm for image encryption based on DNA encoding and multi-chaotic maps. AEU– Int. J. Electron. Commun., 68:3 (2014) 186–192.

[83] P. Gholve and H. A. Hingoliwala, Lossless and Reversible Data Hiding in Asymmetric Cryptography. Int. J. Sci. Res., 4:12 (2015) 1984–1987.

[84] N. R. Zhou, T. X. Hua, L. H. Gong, D. J. Pei and Q. H. Liao, Quantum image encryption based on generalized Arnold transform and double random-phase encoding. Quantum Inf. Process., 14:4 (2015) 1193–1213.

[85] K. Muhammad, J. Ahmad, M. Sajjad and M. Zubair, Secure Image Steganography Using Cryptography and Image. Arxiv abs, (2015) 1–22.

[86] X. Li, Z. Xie, J. Wu and T. Li, Image Encryption Based on Dynamic Filtering and Bit Cuboid Operations. Complexity, (2019).

[87] X. Chai, X. Fu, Z. Gan, Y. Lu and Y. Chen, A color image cryptosystem based on dynamic DNA encryption and chaos. Signal Processing, 155 (2019) 44–62.

[88] D. Nofriansyah et al., A New Image Encryption Technique Combining Hill Cipher Method, Morse Code and Least Significant Bit Algorithm. J. Phys. Conf. Ser., 954:1 (2018).

[89] K. Joshi and R. Yadav, A new LSB-S image steganography method blend with Cryptography for secret communication. ICIIP 2015 - 3rd Int. Conf. Image Inf. Process, (2016) 86–90.

[90] C. A. Sari, E. H. Rachmawanto and E. J. Kusuma, Good Performance Images Encryption Using Selective Bit T-Des on Inverted Lsb Steganography. J. Ilmu Komput. dan Inf., 12:1 (2019) 41.

[91] S. Usha, G. A. S. Kumar and K. Boopathybagan, A secure triple level encryption method using cryptography and steganography. ICCSNT 2011-Int. Conf. Comput. Sci. Netw. Technol., 2 (2011) 1017–1020.

[92] Z.E. Dawahdeh, S.N. Yaakob, R.R. bin Othman, A new image encryption technique combining Elliptic Curve Cryptosystem with Hill Cipher. Journal of King Saud University – Computer and Information Sciences, 30:3 (2018) 349–355.

[93] J. S. Khan and J. Ahmad, Chaos based efficient selective image encryption. Multidimens. Syst. Signal Process., 30:2 (2019) 943–961.

[94] M. Prakash, P. Balasubramaniam and S. Lakshmanan, Synchronization of Markovian jumping inertial neural networks and its applications in image encryption. Neural Networks, 83 (2016) 86–93.

[95] L. Gong, X. Liu, F. Zheng and N. Zhou, Flexible multiple-image encryption algorithm based on log-polar transform and double random phase encoding technique. J. Mod. Opt., 60:13 (2013) 1074–1082.

[96] M. Sharifzadeh, C. Agarwal, M. Salarian and D. Schonfeld, A New Parallel Message-distribution Technique for Cost-based Steganography. Arxiv abs, (2017) 3–7.

[97] B. Oktavianto, T. W. Purboyo and R. E. Saputra, A proposed method for secure steganography on png image using spread spectrum method and modified encryption. Int. J. Appl. Eng. Res., 12:21 (2017) 10570–10576.

[98] Y. Chen, S. Chien and H. Lin, True Color Image Steganography Using Palette and Minimum Spanning Tree. WSEAS Transactions on Computers, (2009) 273–278.

[99] J. Wu, X. Liao and B. Yang, Color image encryption based on chaotic systems and elliptic curve ElGamal scheme. Signal Processing, 141 (2017) 109–124.

[100] Bost, Raphael, Raluca A. Popa, Stephen Tu and Shafi Goldwasser, Machine Learning Classification over Encrypted Data. IACR Cryptol., 331 (2015) 8–11.

[101] R. Das and T. Tuithung, A novel steganography method for image based on Huffman Encoding. Proc. - 2012 3rd Natl. Conf. Emerg. Trends Appl. Comput. Sci. NCETACS-2012, (2012) 14–18.

[102] P. Singh and P. K. Singh, Image Encryption and Decryption. International Journal of Scientific & Engineering Research, 4:7 (2013) 150–154.

[103] Z. Gan, X. Chai, M. Zhang and Y. Lu, A double color image encryption scheme based on three-dimensional brownian motion. Multimed. Tools Appl., 77:21 (2018) 27919–27953.

[104] A. Abusukhon, M. N. Anwar, Z. Mohammad and B. Alghannam, A hybrid network security algorithm based on Diffie Hellman and Text-to-Image Encryption algorithm. J. Discret. Math. Sci. Cryptogr., 22:1 (2019) 65–81.

[105] X. Wang, L. Feng and H. Zhao, Fast image encryption algorithm based on parallel computing system. Inf. Sci. (Ny)., 486 (2019) 340–358.

[106] J. B. Lima, E. A. O. Lima and F. Madeiro, Image encryption based on the finite field cosine transform. Signal Process. Image Commun., 28:10 (2013) 1537–1547.

[107] Y. Zhou, W. Cao and C. L. Philip Chen, Image encryption using binary bitplane. Signal Processing, 100 (2014) 197–207.

[108] L. D. Singh and K. M. Singh, Image Encryption using Elliptic Curve Cryptography. Procedia Comput. Sci., 54 (2015) 472–481.

[109] S. J. Shyu, Image encryption by multiple random grids. Pattern Recognit., 42:7 (2009) 1582–1596.

[110] M. K. Meena, S. Kumar, and N. Gupta, Image Steganography tool using Adaptive Encoding Approach to maximize Image hiding capacity. Soft Comput., 2 (2011) 7–11.

[111] Andysah Putera Utama Siahaan, RC4 Technique in Visual Cryptography RGB Image Encryption. SSRG International Journal of Computer Science and Engineering, 3:7 (2016) 1-6.

[112] K. Ma, W. Zhang, X. Zhao, N. Yu and F. Li, Reversible data hiding in encrypted images by reserving room before encryption. IEEE Trans. Inf. Forensics Secur., 8:3 (2013) 553–562.

[113] S. Dey, SD-AEI: An advanced encryption technique for images:An advanced combined encryption technique for encrypting images using randomized byte manipulation. ICDIPC 2012–2nd Int. Conf. Digit. Inf. Process. Commun., (2012) 68–73.

[114] B. D. Parameshachari, K. M. S. Soyjaudah and D. K. A. Sumitrha, Secure Transmission of an Image using Partial Encryption based Algorithm. Int. J. Comput. Appl., 63:16 (2013) 33–36.

[115] M. L. Piao, Z. X. Liu, Y. L. Piao, H. Y. Wu, Z. Yu and N. Kim, Multi-depth three-dimensional image encryption based on the phase retrieval algorithm in the Fresnel and fractional Fourier transform domains. Appl. Opt., 57:26 (2018) 7609.

[116] N. Rahim, J. Ahmad, K. Muhammad, A. K. Sangaiah and S. W. Baik, Privacy-preserving image retrieval for mobile devices with deep features on the cloud. Comput. Commun., 127 (2018) 75–85.

[117] S. K, An Optimal RSA Encryption Algorithm for Secret Images. Int. J. Pure Appl. Math., 118:20 (2018) 2491–2500.

[118] K. Madhusudhan Reddy, A. Itagi, S. Dabas and B. K. Prakash, Image encryption using orthogonal Hill Cipher algorithm. Int. J. Eng. Technol., 7:4 (2018) 59–63.

[119] S. Hemalatha, U. D. Acharya, A. Renuka and P. R. Kamath, A Secure and High Capacity Image Steganography Technique. Signal Image Process. An Int. J., 4:1 (2013) 83–89.

[120] S. Tedmori and N. Al-Najdawi, Image cryptographic algorithm based on the Haar wavelet transform. Inf. Sci. (Ny)., 269 (2014) 21–34.

[121] Y. Bassil, Image Steganography based on a Parameterized Canny Edge Detection Algorithm. Int. J. Comput. Appl., 60:4 (2012) 35–40.

[122] R. G. Zhou, Q. Wu, M. Q. Zhang and C. Y. Shen, Quantum Image Encryption and Decryption Algorithms Based on Quantum Image Geometric Transformations. Int. J. Theor. Phys., 52:6 (2013) 1802–1817.

[123] M. A. Albahar, O. Olawumi, K. Haataja and P. Toivanen, a Novel Method for Bluetooth Pairing Using Steganography. 9 (2017) 53–66.

[124] M. Moradi and M.-R. Sadeghi, Combining and Steganography of 3D Face Textures. JECEI, 3 (2017) 3–8.

[125] A. Mehndiratta, Data Hiding System Using Cryptography &; Steganography: A Comprehensive Modern Investigation. Int. Res. J. Eng. Technol., 2:1 (2015) 2395–56.

[126] K. Kaur and N. Garg, Data Storage Security Using Steganography Techniques. Int. J. Tech. Res. Appl., 4:6 (2016) 93–98.

[127] B. S. H. Kumar and D. R. V. U. S. H. A. S. Hree, Encrypting Images by Patch-Level Sparse Representation for High Capacity Reversible Data Hiding. International Journal of Advanced Technology and Innovative Research, 9:1 (2017) 1–8.

[128] P. Bas, Natural Steganography: cover-source switching for better steganography. Arxiv Labs, (2016) 1–13.

[129] M. J. Pelosi, G. Kessler, M. S. S. Brown and G. Kessler, One-Time Pad Encryption Steganography System. CDFSL, (2016).

[130] V. Holub, J. Fridrich and T. Denemark, Universal distortion function for steganography in an arbitrary domain. Eurasip J. Inf. Secur., (2014) 1–13.

[131] A. A. Abu Aziz, H. N.Qunoo, and A. A. Abu Samra, Using Homomorphic Cryptographic Solutions on E-voting Systems. Int. J. Comput. Netw. Inf. Secur., 10:1 (2018) 44–59.