

International Journal of Informatics and Applied Mathematics
e-ISSN:2667-6990 Vol. 4, No. 1, 28-55

Evolutionary Encryption Algorithm Ensuring Privacy in Video Surveillance

Yakouta Zarouk¹, Ismahane Souici^{1,2}, Samir Hallaci¹, and Hamid Seridi¹

¹ LabSTIC, 8 mai 1945 University, Guelma, Algeria, 24000
(zarouk.yakouta, hallaci.samir, seridi.hamid)@univ-guelma.dz

² LAOTI, Mohamed Seddik Ben Yahia University, Jijel, Algeria, 18000
souici.ismahane@yahoo.fr

Abstract. The widespread use of video surveillance and the development of embedded information processing systems raise the issue of affecting the confidentiality and integrity of video data and even the individuals privacy. In order to secure the content of video and protect the public privacy, we propose a new system for detecting and encrypting regions of interest (ROIs). The ROI detection is based on an improved Gaussian mixture model where we use supervisors to control the changes in the image. The regions of interest encryption is performed through the use of an enhanced evolutionary encryption algorithm, exploiting the representation of the RGB color space to get real time system. Results and comparisons presented in this paper show that the proposed scheme can effectively detect and obscure the identity of people to achieve the privacy protection.

Keywords: Video Encryption · Encryption Algorithm · Evolutionary Algorithm · Region of Interest · Gaussian Mixture Model · Video Surveillance.

1 Introduction

Nowadays, video surveillance is one of the ubiquitous multimedia services in our daily life and plays an important role in securing goods and people. Moreover, the rapid development of Information and Communication Technology (ICT) facilitates the storage and transmission of video data between cameras and monitoring stations. This raises the problem of the data content exposure to hacking or malicious use [29]. The increasing uses of video surveillance in both the public and the private sectors, as well as the development of embedded information systems such as identification and recognition of people systems raise the issue of privacy violation. From these facts, data security becomes a major concern [28, 40] to ensure the confidentiality, the integrity of these data and preserve the privacy [44], which is the subject of our paper.

To overcome this problem, cryptography is the most effective tool to address the needs of information security. Indeed, researchers have proposed algorithms for video encryption using standard encryption algorithms such as DES [52] and AES [9]. These systems are not suitable for encrypting video for their massive volume.

In order to meet the needs and requirements posed by multimedia applications such as: the encryption effectiveness, the compression efficiency, the privacy protection and the calculation speed; researchers have turned to the characteristics and content of the video data to provide selective or/and partial video encryption algorithms by selecting and encrypting sensitive parameters or sensitive areas.

In this perspective we propose a new system based on two enhanced algorithms to protect sensitive regions of interest privacy in video surveillance applications. First, for detecting the regions of interests (ROI), we propose an improved Gaussian mixture model (GMM) to eliminate local variations using supervisors which control the changes in the homogenous areas. Second, we encrypt ROI using our proposal enhanced version of the evolutionary encryption algorithm [49] OEEA (Occurrences based Evolutionary Encryption Algorithm), exploiting the representation of the RGB color space to get a reduced computation time. Our objective is to achieve: the security needs, privacy protection, the compression ratio conservation and the real time recommendation in video surveillance system.

The rest of this paper is organized as follows: the second section presents a state of the art on the different models of video encryption algorithms, and the third section is dedicated to the description of the different phases of our proposed system. The experimental results and interpretation are presented in the fourth section. Finally, we close with a conclusion.

2 State of the art

In recent decades, many methods and techniques based on cryptography were proposed to address the security needs of video data. In the first preview of

video encryption algorithms, the researchers focused on conventional encryption algorithms [48] such as DES and AES mainly exploiting permutations and substitutions. These algorithms provide the highest level of security, but treat the video as a text or binary string. However, these techniques cause a high computational time which is not suitable for video surveillance systems in real time. Other methods have been developed exploiting different techniques, among others we find the chaotic principles used alone [35, 61, 56, 53] or coupled with other techniques [2, 55], where in [2] cellular automata and selective encryption of quantized Discrete Cosine Transform (DCT) coefficient were used to develop a new scheme for joint compression and encryption of digital images and [55] proposed a novel spatiotemporal chaos model (MCML) by mixing Logistic, Sine and Tent maps into CML map together.

At the same time and with the advancement of cloud computing and fog computing leading to the displacement of storage and processing of data, especially videos, from local servers to fog and cloud; security issues have drawn wide attention. To answer it, many works have been carried out such as [24] which proposed a cloud-fog-local video encryption which consists of a three-layer service model and corresponding key management strategies, a fine-grain video encryption algorithm based on the network abstract layer unit (NALU), and a massive video encryption framework based on Spark. [27] ensures the principle of confusion/diffusion and that of automated-selection mechanism.

Thus and for the reasons explained above, the research has been directed towards the characteristics of the video. One of the most exploited factors is the DCT coefficients. Where, the authors exploit the DCT coefficients representation to scramble them [54, 59] or to encrypt their sign bits by an encryption algorithm [47]. These techniques can save a lot of overhead compared to conventional encryption algorithms, but they cause an increase in video size. Another factor used is the Huffman table in MPEG videos [57, 12] or CAVLC / CABAC in H.264/AVC videos [45] or in HEVC videos [46]. The encryption process is applied within the entropy coding. Other algorithms take into consideration the properties of the compressed video, such as the relationship between I (Intra-coded picture) and P (Predicted picture) / B-frame (Bidirectional predictive picture), and the uniform distribution of byte values in a compressed video [1, 58]. These techniques offer a good level of security and preserve syntax and compression ratio.

The mentioned approaches above are considered as selective encryption methods, where only a few data are encrypted instead of the entire video. They guarantee a reduced processing time and a good level of security. Though they achieve privacy protection, there is a problem for the security guards who cannot see intelligibly the video surveillance.

Therefore, studies have been proposed so that the video surveillance rests intelligible while preserving the individuals privacy. These approaches include detecting the regions of interest (ROI)[42] and then encrypt them using efficient encryption algorithm in time and complexity. These techniques are called partial encryption video algorithms. Bolt [3], Rodrigues et al. [41] and Hong

et al. [21] proposed systems to protect privacy by hiding faces using conventional encryption algorithms. Thus, the effectiveness of each proposed system is based on the robustness of the detection method. In [41] and [21], the detection technique is based on skin color detection which provide false detection of face and a long computation time [21]. Meibing et al. [32] presented a technique for faces protection based on Bayes classifier for detecting ROI and Kalman filter for tracking. The encryption step is done within entropy coding CABAC, where they encrypt each nonzero RC block by two atomic operations RCME (Regular Coding Mode Encryption) and BCME (Bypass Coding Mode Encryption). This proposal achieves the privacy protection but it has a high computational complexity. Rahman et al. [39] proposed a system to hide sensitive information. They calculate ROI with an existing method for face recognition [38] which is based on Eigen faces and principal component analysis (PCA). This method is sensitive to illumination variations. For ROI encryption they use the chaos cryptography technique. This proposal provides a computationally efficient, however it is not suitable for large scale for video surveillance. Zhang et al. [60] presented an approach to privacy protection in the public sector, using the encryption method proposed by Dufaux and Ebrahimi [11] where they flip the signs of the DCT coefficients of ROI pseudo randomly. The effectiveness of the method in [60] is based on the proposed improvement, where they incorporate semantic information of each detected observation [25] in a Markov chain model with two hidden states. Based on FMO (Flexible Macroblock Ordering) technology, Peng et al. [36] proposed a scheme for ROI privacy protection by a selective encryption on CAVLC encoding using chaos cryptography. The ROI detection is based on the detection of the skin color by using the proposed method by Rein et al. [22]. This latter is sensitive to light condition which affects the detection rate. To protect personal privacy in H.264 video Guo et al. [20] proposed a selective encryption scheme. Human face regions are selected as ROIs and detected using Gaussian skin model [7]. However, this technique needs a classifier for decreasing the negative detection rate. The authors in [20] have exploited the representation of FMO in H.264, where each frame is mapped into different slice groups. Different slice groups can be chosen flexibly to form desirable ROI in each frame. The encryption process is carried out by exclusive OR (XOR) operation between a secret key and DC coefficients of luminance component and inverting signs of chrominance DC coefficients. Table 1 summarizes the comparative analysis of partial video encryption methods.

From Table 1 we note that the partial video encryption algorithms provide a certain level of security, but the balance between security and the overall performance is still a problem. The ROI detection algorithms have weaknesses that affect the encryption algorithm efficiency such as the computation time, noise sensitivity and false detections.

In the present work, we focus on the two parts of the partial video encryption system. For ROI detection, we propose an improvement of Gaussian mixture model, which is robust to the problems of luminosity variations and offers a fast execution time. In order to have an effective and secure video surveillance

Table 1. Comparative analysis of partial video encryption schemes.

Authors	Encryption Algorithm	Security weaknesses	Detection Algorithm	Detection Weaknesses
Boult [3]	AES, 3DES	- High computation time. - Block size consideration. - Attacks on 3DES.	Viola and Jones (Open CV)	- Long time for training.
Rodrigues et al. [41]	AES with OFB mode	-High computation time.	Detection	-False detection.
Hong and Jung [21]	AES, DES	- High computation time. - Block size consideration. - Attacks on DES.	MLP and Gaussian model for skin color	- High computation time. - No detection in multi scale.
Meibing et al. [32]	RCME and BCME	- High computational complexity.	Bayses classifier and tracking by Kalman filter	- False detection. - High computation time.
Rahman et al. [39]	Chaos cryptography	- High computation time in large scale.	Eigenfaces and PCA [38]	- Sensitive to uncontrolled illumination. - False detection.
Zhang et al. [60]	Flipping the signs of the DCT coefficients [11]	- Differential attack not discussed.	Detection and tracking by a model of chain	- High computational complexity.
Peng et al. [36]	Chaos cryptography	- High computation time in large scale.	Face Recognition based on skin color [22].	- Sensitive to light condition. - False detection.
Guo et al. [20]	Pseudo Random Number Generator and XOR operation	-Vulnerable to known plain text attack	Gaussian skin color model [7].	-False detection -Computation time

system, we propose an enhanced evolutionary encryption algorithm EOEEA to deal with various cryptanalysis attacks and to be applicable in real time system.

3 Proposed method

We propose a new efficient partial encryption algorithm to protect regions of interest (ROI). In video surveillance systems human and moving objects are possible ROIs[33, 34]. The proposed method consists of two main steps: detection and encryption of the ROI. Fig 1 illustrates the general architecture of the system.

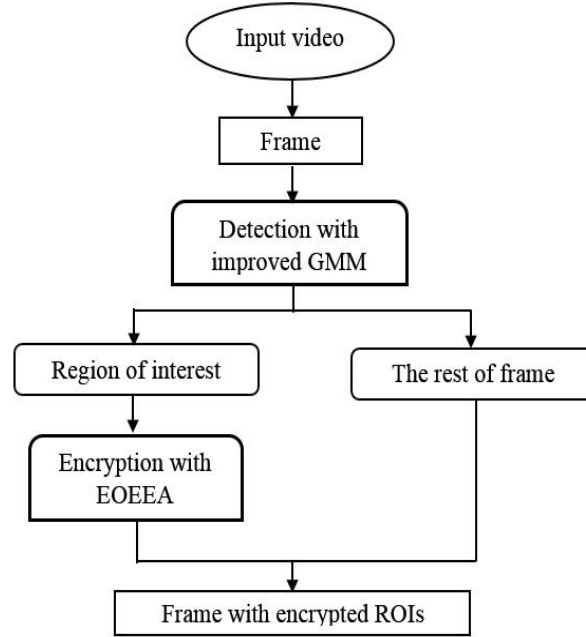


Fig. 1. Schematic description of the proposed system.

3.1 Region of interest Detection

In this step of our system, region of interest detection is carried out by a method of background subtraction in a video. Modeling background with Gaussian Mixture Model (GMM) is the most widely used method due to its performance. However, this technique is sensitive to the local variations and illumination changes [4, 15]. In this context, many improvements of GMM have been proposed over the recent years. Farou et al. [5] proposed an interesting technique to overcome these problems. They divide the first captured frame into several equal size zones, each zone will be assigned to a supervisor that can calculate its histogram and store it. For each new frame, the supervisor can detect changes in the area by calculating the degree of similarity between the actual calculated histogram and the stored one. If the supervisor detects a change in the area an update is done for the GMM parameters of these zones pixels.

This intuitive division cannot effectively express the actual changes in each area[16]. Indeed, a histogram records only the distribution of colors in the image whereas images with different appearances can have similar histograms Fig.2. Furthermore the number of regions in Farou et al. proposal [5] is defined empirically depends on the scene nature of the image.

For these reasons, we propose an improvement by dividing the frame into a set of homogeneous zones to express the effect of the change on the histogram



Fig. 2. Two images with similar histograms.

based on HSV color space [14]. To obtain these homogeneous zones, we can use an image segmentation technique. Hence, the number of zones is automatically obtained.

The pseudo code in Algorithm 1 depicts the different steps of the proposed algorithm:

Algorithm 1 : Improved GMM algorithm

Initialization:

Split the first captured frame into several homogenous zones
 Convert all the pixels of the frame from RGB format to HSV format;
 Assign a supervisor to each area;
 Calculate and store the color histogram of each zone based on the component V;
 Initialize the parameters of the GMM;

Iteration:

for each new frame **do**
 Convert all the pixels of the frame from RGB format to HSV Format
 for each zone **do**
 Calculate the color histogram by the supervisor based on the component V;
 Measure the degree of similarity between the calculated histogram and the stored one;
 if the difference is greater than a threshold T **then**
 Save the new histogram;
 Update parameters of GMM;
 end if
 end for
end for

Initialization phase In this first phase, we aim to initialize the proposed algorithm parameters. The first step is to divide the first captured frame into homogeneous regions. Region growing segmentation algorithm is a straightforward and effective approach for color image segmentation. It starts from selected pixels (seeds) representing distinct image regions and to grow them according to a homogeneity criterion, until they cover the whole image. The seed points can be selected either manually or automatically. In this paper, we have used an improved version of region growing segmentation algorithm [8]. The segmentation result is a number of distinct regions, the next step is to assign each one a supervisor, which is a thread that calculate the histogram of the area and memorize it. The multithreaded processing helps us to accelerate the treatment. The final step of this phase is the initialization of GMM parameters which will be detailed in the next section.

Iteration phase The result of this phase is regions of interest location which will serve as the second part of our system. For each new frame, the supervisor can detect changes in the region by calculating and comparing the degree of similarity between the stored histogram and the current one. The Bhattacharyya coefficient is a measure of similarity that we used[17]. It defines a normalized distance between two discrete probability distributions [23]. For two probability distributions p and q The Bhattacharyya coefficient is defined by Eq. (1):

$$BC(p, q) = \sum_{x \in X} (\sqrt{p(x) \cdot q(x)}) \quad (1)$$

BC is between 0 and 1 which helps us to easily choose a threshold T where, if BC is greater than this latter the supervisor saves the current histogram and indicates a signal to update the GMM parameters. Modeling background by GMM have known many improvements since the publication of the original method proposed by Stauffer and Grimson [51]. In our paper, we have used a variant of GMM proposed by Charoenpong et al. [6, 13]. Each pixel is modeled by K Gaussian distributions. The probability of observation the current pixel value is:

$$p(X_t) = \sum_{i=1}^k (\omega_{i,t} \cdot f(X_t | u_{i,t}, \Sigma_{i,t})) \quad (2)$$

Where k is the number of Gaussians, $\omega_{i,t}$, $u_{i,t}$ and $\Sigma_{i,t}$ are respectively the weight, mean value and covariance matrix of the i^{th} Gaussian in time t and f is a Gaussian probability density function represented by (3):

$$f(X_t | u_k, \Sigma_k) = \frac{1}{(2\pi)^{n/2} |\Sigma_k|^{1/2}} e^{-\frac{1}{2}(X_t - u_k)^T \Sigma_k^{-1} (X_t - u_k)} \quad (3)$$

After reporting the change in the region by its supervisor, an update of GMM parameters ($\omega_{i,t}$, $u_{i,t}$ and $\Sigma_{i,t}$) of the regions pixels is done using the method described in [6], based on the numbers of Gaussians(k), the learning rate (α) and

the measure of the minimum portion (β) which are initialized in the first phase of the algorithm. The last step of the algorithm is to subtract the background and detect the ROIs by determining whether the pixel belongs to the foreground or to the background. Figure 3 represent the result of GMM procedure.

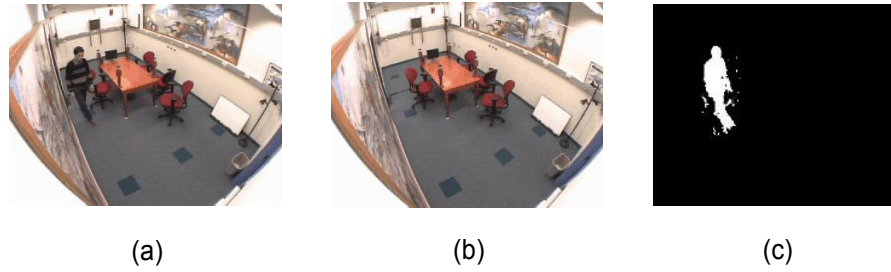


Fig. 3. GMM procedure: (a) The input video, (b) The background, (c) ROI detection.

3.2 Region of Interest Encryption

The problem of encryption can be reduced to an optimization problem [50] where we aim to maximize the difference between the encrypted data and its original version. Genetic algorithms have proved their efficiency and adaptability to any search space to solve this type of problem. Souici et al. [49] have used the genetic algorithms evolutionary-principle to propose an Occurrences based Evolutionary Encryption Algorithm OEEA. The proposed method is based on the representation of the pixel intensities occurrences in the RGB color space. Indeed, the initial chromosome is composed of 768 genes (Fig. 4). However this proposal generate a high computation time which is not appropriate for video surveillance system.

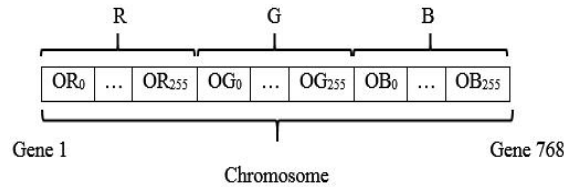


Fig. 4. Coding of individuals in OEEA.

In order to decrease the computational time, we exploit the independence of RGB color space components to propose a reduced representation of the chro-

mosome, where we separate the three components of the color space into three chromosomes (ORI, OGI and OBI), each with a size of 256 genes (In order to decrease the computational time, we exploit the independence of RGB color space components to propose a reduced representation of the chromosome, where we separate the three components of the color space into three chromosomes (ORI, OGI and OBI), each with a size of 256 genes (Fig. 5). In addition, we exploit this representation to get a parallel processing.

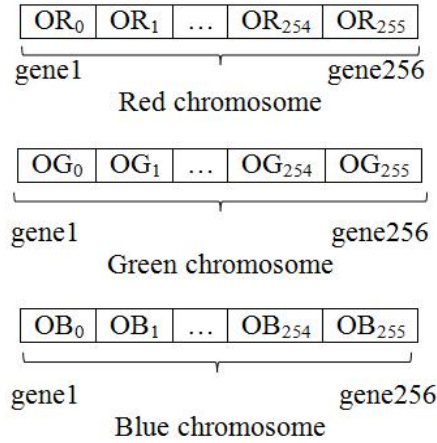


Fig. 5. Coding of individuals in each population in EOEEA.

Algorithm 2 illustrates the process of the Enhanced Occurrences based Evolutionary Encryption Algorithm EOEEA:

Algorithm 2 : EOEEA Algorithm

Initialization:

Calculate the initial chromosomes OR_0 , OG_0 and OB_0 ;
 Generate the initial populations (PopR, PopG and PopB);
 Define the reproduction thread;

Iteration :

repeat

 Reproduction(PopR).start;
 Reproduction(PopG).start;
 Reproduction(PopB).start;

until stopping criterion

Reconstruct encrypted image using the best found solutions.
 Generate the encryption key

Encryption process: Genetic algorithms are based on the evolution principle, where they combine genetic reproduction operators (crossover, mutation and selection) knowing that a population has a number of individuals (chromosomes) experimentally determined in order to find the best solution to a problem.

The first step in the genetic algorithms is to generate an initial population. In our proposal, three populations are generated by applying slight random perturbations. The n individuals of each initial population are obtained by swapping genes randomly of the chromosomes. Fig.6 shows the operating principle of EOEEA.

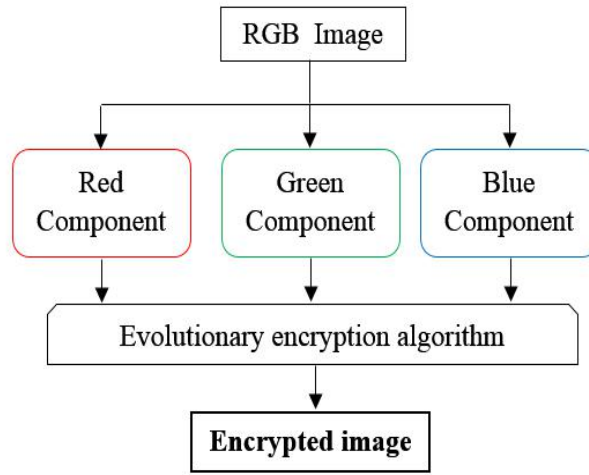


Fig. 6. Operating principle of EOEEA.

The evolutionary process represents the cryptographic process. To get the encrypted versions of the components RGB, we apply the reproduction process on each population where we seek the best individual that is different from the initial chromosome. In this case, our objective is to maximize the fitness function defined in Eq. (4):

$$f(ch) = \sum_{i=1}^{256} (|ch_i - chI_i|) \quad (4)$$

Where: $ch = OR, OG, OB$; $chI = ORI, OGI, OBI$.

◆ *Reproduction Process*

This phase of the algorithm ensures the new individuals reproduction of each population, by applying the following genetic operators:

a) Crossover

This operator is based on the coupling of two parents randomly selected. In our case, we chose the crossover of two chromosomes proposed by Davis [10] in order to have more diversity between a generation and the other.

b) Mutation

It consists of locally modifying an individual to reproduce a new one. In our algorithm, we apply a simple permutation of two genes randomly chosen from the chromosome with a fixed rate experimentally.

c) Selection

The purpose of selection is to ensure the survival of the best elements across generations. In our case, we chose the proportional selection that involves inserting new individuals in the population, then sort them in order to conserve the best individuals.

As our design is built around three independent populations, the process of reproduction of three populations will run on different threads so they can be executed in parallel to reduce the processing time.

To ensure the convergence of our algorithm, the reproduction process will be iterated until a stopping criterion is verified, which is defined as follows:

$$\begin{aligned} (0 < F(OR) < 255) \text{ and} \\ (0 < F(OG) < 255) \text{ and} \\ (0 < F(OB) < 255) \end{aligned} \quad (5)$$

The result of the cryptographic process is three color components (Red, Green and Blue) encrypted independently. From these, the encrypted image will be rebuilt.

◆ *Key generation*

The final step serves to generate the encryption key of each component RGB. In our case, we obtain three session keys where each key is obtained by exploiting the original component and its encrypted version. Each session key represents the permutations of pixels-occurrences positions forming the encrypted component to obtain the pixels-occurrences positions forming the original component. The final key is the concatenation of these three session keys (encryption key of the Red component, encryption key of the Green component and encryption key of the Blue component).

Decryption process: The output from the previous steps is a video where regions of interests are encrypted with the algorithm described above. Deciphering is to reconstruct the original video from the encrypted video. This process is composed of two steps: the first step serves to extract the coordinates of the regions of interest (ROIs) which are recorded in the detection step of our system. The second step is to introduce by the appropriate key for each ROI. This

latter allows reproducing the appropriate permutations for each ROI encrypted for each image in order to have the original video.

4 Experimental results and interpretation

The algorithms presented in this paper are implemented in Java on a computer with an Intel Core (TM) i3 3.30 GHz processor and 4GB of memory capacity. To demonstrate the performance of the proposed methods, experiments were carried out on a variety video sequences in different environments and conditions (resolution, illumination variations, scale changes), where we have used: laboratory and intelligent room [37], hall, Bootstrap and shopping mall [26], hallway [31] and a standard video Hall monitor. Some detection and encryption results are shown in Figure 7 and 8.

To evaluate the proposed scheme performance such as: efficiency of ROI detection method, compression performance, computational time and security are analyzed as follow.

4.1 ROI detection algorithm efficiency

This section contains some experimental results for moving objects which are defined as regions of interest in our paper. The results of ROIs detection with our proposal are compared with the GMM proposed in [6] and the proposal by Farou et al. [5]. The GMM parameters have been fixed for each experiment, the choice of the numbers of Gaussians (k), the learning rate (α) and the measure of the minimum portion (β) depends on the complexity of video. In our proposal, the number of zones in the initialization phase depends on the result of the region growing segmentation algorithm. On the other hand, in the proposal of Farou et al. [5] the zones number is empirically obtained for each video.

Table 2 shows that the proposed improvement of GMM eliminates more the problem of local variations comparing to that proposed by Farou et al [5].

To evaluate the performance of our proposed improvement of GMM, statistical information was used such as detection rate DR Eq. (6) and false alarm rate FAR Eq. (7) [18]:

$$DR = \frac{TP}{TP + FP} \quad (6)$$

$$FAR = \frac{FP}{TP + FP} \quad (7)$$

True Positive (TP): the number of foreground pixels correctly detected.

False Positive (FP): the number of background pixels incorrectly detected as foreground pixels (also known as false alarms).

Table 3 shows the results of the comparison between GMM proposed in [6], Farou et al. proposal[5] and our proposed method.

Table 2. Comparison results between GMM proposed in [6], Farou et al. proposal [5] and our proposal


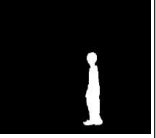

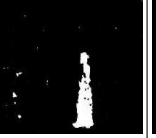
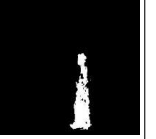


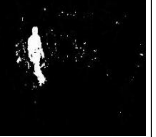

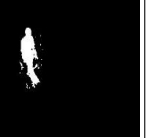

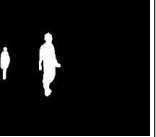

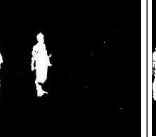




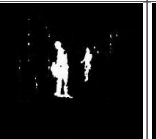

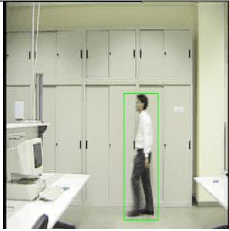





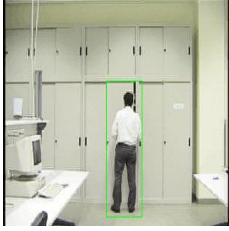
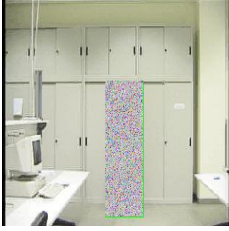
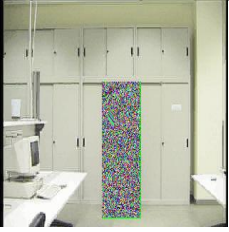



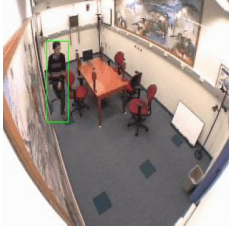

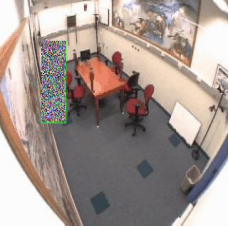
Video (Frame)	Original frame	Ground Truth	GMM [6]	Farou et al. Proposal [5]	Our Proposal
Laboratory (153)					
Intelligent room (249)					
Hallway (407)					
Hall monitor (44)					

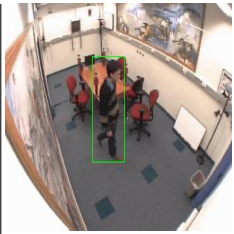
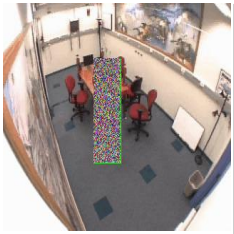
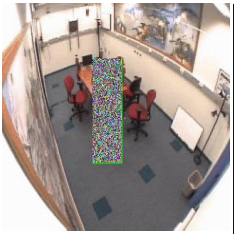


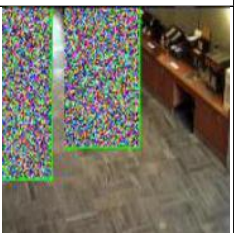




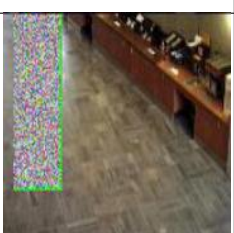
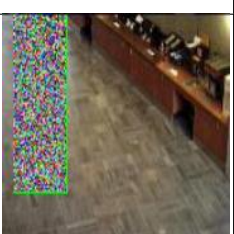
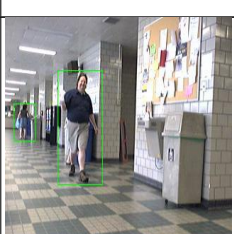
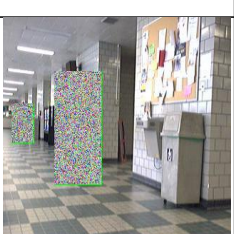
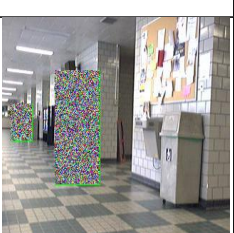
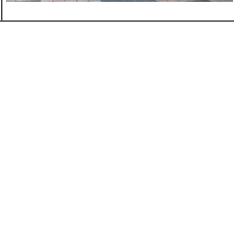
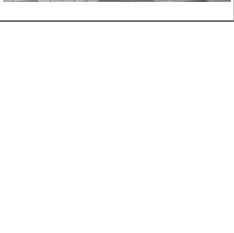
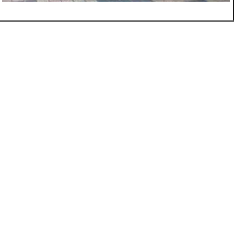
Table 3. Comparison DR and FAR between GMM proposed in [6], Farou et al. [5] proposal and our proposal.

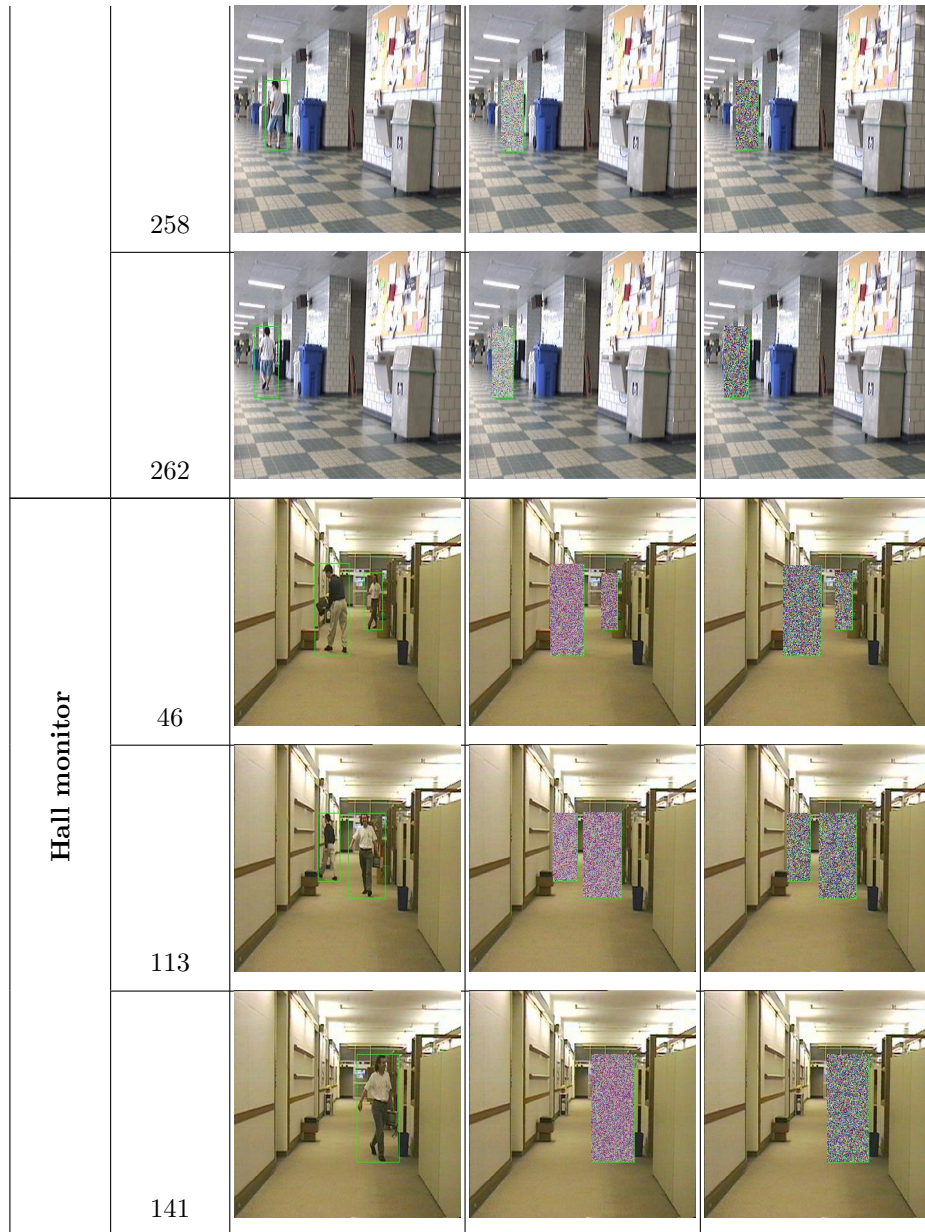
Video	GMM [6]		Farou et al. proposal [5]		Our proposal	
	DR	FAR	DR	FAR	DR	FAR
Laboratory	0.6578	0.3422	0.7873	0.2127	0.8202	0.1798
Intelligent room	0.6955	0.3045	0.7874	0.2126	0.8126	0.1874
Hallway	0.7943	0.2057	0.8433	0.1567	0.8425	0.1575
Hall monitor	0.8161	0.1839	0.9031	0.0919	0.9300	0.0700

From Table 3, we can see that the GMM proposed in [6] gives the upmost total of false alarm rate, while our proposal provide a highest detection rate and lowest false alarm rate. Table 4 shows the effectiveness of the proposed method to detect multi regions of interest whatever the illumination conditions in different environments, while maintaining the same computational resources.

Table 4: Results of the region of interest detection and encryption.

Video	Frame number	Detection results with our proposal	Encryption results	
			EOEEA	AES
Laboratory	153			
	281			
	299			
Intelligent room	204			
	240			

				
Bootstrap	275			
	220			
	276			
	295			
Hallway	184			



4.2 Proposed encryption algorithm efficiency

The genetic algorithms effectiveness is based on the appropriate choice of its parameters. Adjustment of these parameters is often done approximately through experiments [19]. In order to have the appropriate parameters of our algorithm,

we performed our experiments on several videos. The table 5 shows the final parameters adopted.

Table 5. The adopted parameters

Parameters	Adopted value
Population size	15
Number of generations	30
Mutation rate	0,7

In order to achieve the need for a high level of security and a reduced time, we studied the relationship between the convergence value (CV) which represents the algorithm confusion, the number of generations and the run time. To demonstrate effectively these relationships, we performed experimental studies on the Lena image (302x302 pixels). The results are shown in Fig. 7 and Fig. 8. From the figures, we note that the generation number influences on the CV and the computational time. For this reason, we made a trade-off between convergence value CV and the run time and we have adopted the parameters presented in the table 5.

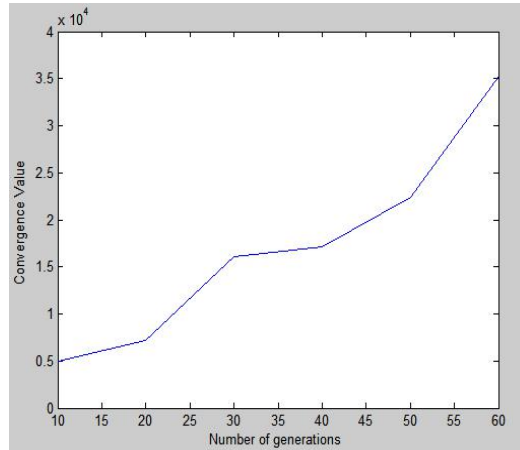


Fig. 7. Influence of the number of generations on the convergence value.

Furthermore, this computation time is varied depends on the image size. In our case, we encrypt ROIs only, which gives a computational time more reduced.

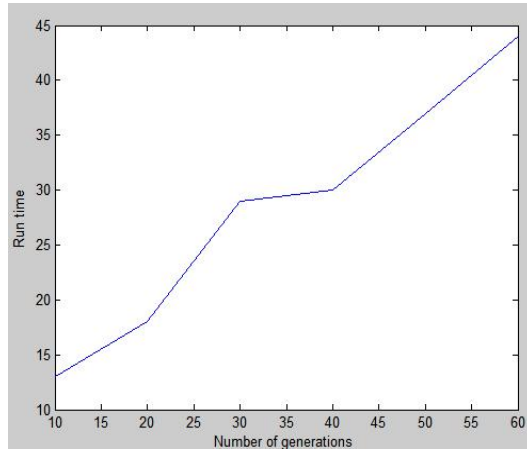


Fig. 8. Influence of the number of generations on the run time (ms).

Compression performance In video surveillance systems, maintaining a good compression ratio is a necessary requirement in the process of storage and transmission data. In our system, video encryption is independent of its compression. Thus, the final result of the system (ROI detection and encryption) is subjected to MPEG-4, or any other video compression algorithm.

For comparing the compression performance of each implemented video encryption algorithm, we have used compression ratio Δr defined as follow:

$$\Delta r = \frac{(r_2 - r_1)}{r_1} \times 100 \quad (8)$$

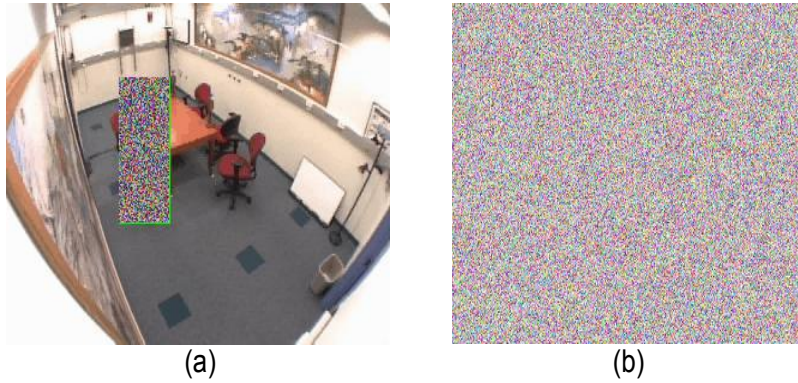
Where r_1 represents the data volume of the video before encryption and r_2 represents the data volume of the video after encryption. The results are shown in Table 6.

From table 6 above, the size of the bit stream increased a little bit for the encrypted video with EOEEA. The increased data is mainly due to the information redundancy change in the region of interest. However, this increase of the bit stream is still less compared to that obtained in case of the encrypted video with AES. Comparing our proposal to the joint compression and encryption methods [36] that have an overhead of the compression ratio which varies from 5 to 8%, our proposed scheme preserves much better compression efficiency.

Computational time The aim of this proposal is to reduce the computational time of encryption algorithm to be applied to video surveillance applications in real time. Table 7 reports the results of applying the three algorithms on the test videos in terms of average of encryption time per frame (ms). Results

Table 6. Comparison of the variation of compression ratio (Kilo Byte)

Algorithm	Video sequences	Before encryption	After encryption	Overhead Δr (100%)
		r_1	r_2	
EOEEA	Laboratory	44708	44750	0.09
	Intelligent room	44820	44871	0.10
	Hall way	44858	44902	0.11
	Hall	14765	14792	0.18
	Bootstrap	11183	11232	0.43
	Shopping mall	47688	47745	0.12
	Hall monitor	29308	29361	0.18
AES	Laboratory	44708	45121	0.93
	Intelligent room	44820	45201	0.85
	Hall way	44858	45123	0.59
	Hall	14765	14912	0.99
	Bootstrap	11183	11320	1.22
	Shopping mall	47688	47998	0.65
	Hall monitor	29308	29525	0.74

**Fig. 9.** Example of full and partial encryption of the Intelligent room video (frame 229): (a) Partial encryption (b) Full encryption

show that ROIs detection with modified GMM and their encryption consume less computational time than full encryption. Moreover, the video surveillance rests intelligible while individuals privacy is protected (Fig. 9).

The speed of the evolutionary encryption algorithm depends on the used encoding, where the size of this latter is uniform whatever the size of the image. In the case OEEA, coding size is 786 elements, in our proposal this elements number is distributed on three chromosomes of 256 elements each. In addition,

Table 7. Comparison of the encryption times per frame between the partial and full encryption (ms).

Video	Algorithm	EOEEA		OEEA		AES	
		Full	Partial	Full	Partial	Full	Partial
Intelligent room (320x240)		29	11	82	29	105	41
Laboratory (320x240)		25	14	72	39	98	44
Hall way (320x240)		28	15	80	42	102	59
Hall (176x144)		20	12	72	35	92	49
Bootstrap (160x120)		18	9	60	28	88	47
Shopping mall (320x256)		28	13	78	41	96	65
Hall monitor (352x288)		32	17	91	43	112	62

OEEA cannot be treated as a parallelism problem. Therefore, the proposed coding enables the treatment in EOEEA to run in three parallel independent threads. From the experimental results presented in Table 6 we note that the average execution time given by EOEEA is decreased almost by one third compared to OEEA. This fact makes the proposed system EOEEA more appropriate for real-time applications.

Security efficiency In order to ensure confidentiality, integrity of data and the privacy protection, the encryption system must resist different attempted attacks. In this section, we will discuss and analyze the security of the proposed system:

Perceptual security The results obtained with the implemented encryption algorithms show that the regions of interest are completely unintelligible (Table 4). However, the result obtained by AES shows that the regions of interest keep some of their texture because of the block cipher (Fig.10). We can see clearly that encrypted image by AES contains textured zones (Fig.10 (a)), and encrypted image by EOEEA is homogeneous (Fig.10 (b)). Consequently EOEEA provide a high security in perception.

Statistical attack This type of attack considered an encryption system as a black box, where it analyses statistically inputs and outputs of the system. To compare and evaluate the strength of implemented systems against the statistical attacks, we used the following measures on the encrypted region of interest: MAE (Mean

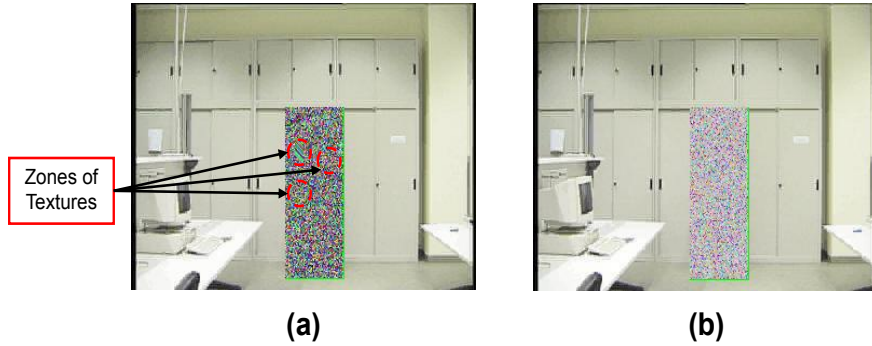


Fig. 10. Example shows that AES kept some texture compared to EOEEA (Frame 299 from laboratory video): **(a)** Encryption with AES, **(b)** encryption with EOEEA.

Absolute Error) and MSE (Mean Square error) which are given respectively by the following expressions:

$$MAE = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N \frac{|Im_0(i, j) - Im_c(i, j)|}{255} \quad (9)$$

$$MSE = \sum_{i=1}^M \sum_{j=1}^N \frac{(Im_0(i, j) - Im_c(i, j))^2}{225^2} \quad (10)$$

Where M and N mean the width and height of the image, $Im_0(i, j)$ and $Im_c(i, j)$ are the original image and the ciphered image respectively.

These measures are used to quantify and evaluate the difference between the original image and the encrypted image. Table 5 shows the average of these measures applied to the test videos encrypted with the three algorithms in order to compare them. The results show a good confusion for the three algorithms. Although EOEEA presents in its entirety good performance compared to other algorithms, the results are quite high and very close to each other for the three cases of figures. This shows the strength of these algorithms against statistical attacks.

Differential attack This attack tries to deduce the operation of an encryption system, by comparing and observing the changes in the cipher data, often by making a small alteration in the plain data [30]. Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are two common quantitative measures, which are defined as:

$$NPCR = \frac{\sum_{i,j} D(i, j)}{M \times N} \times 100\% \quad (11)$$

Table 8. Levels of confusion for test videos.

Video	Algorithm	AES		OEEA		EOEEA	
		MAE	MSE	MAE	MSE	MAE	MSE
Intelligent room (320x240)		1.1456x 10 ⁻⁴	64.4230	1.4243x 10 ⁻⁴	75.7115	1.6347x10 ⁻⁴	73.8755
Laboratory (320x240)		1.2436x10 ⁻⁴	65.2346	1.5764x 10 ⁻⁴	69.2467	1.6768x10 ⁻⁴	76.7689
Hall way (320x240)		1.1544x10 ⁻⁴	70.9043	1.6570x10 ⁻⁴	76.1275	1.7689x10 ⁻⁴	75.9054
Hall (176x144)		1.2453x 10 ⁻⁴	71.5330	1.4356x 10 ⁻⁴	78.0098	1.78347x10 ⁻⁴	74.2345
Bootstrap (160x120)		1.1096x10 ⁻⁴	64.2145	1.5678x 10 ⁻⁴	73.0985	1.89237x10 ⁻⁴	76.0937
Shopping mall (320x256)		1.1756x10 ⁻⁴	67.2189	1.2313x 10 ⁻⁴	72.3457	1.7689x10 ⁻⁴	79.9567
Hall monitor (352x288)		1.1680x10 ⁻⁴	69.4356	1.5678x 10 ⁻⁴	70.7785	1.5467x10 ⁻⁴	77.1730

$$D(i, j) = \begin{cases} 0 & \text{if } C(i, i) = C'(i, j) \\ 1 & \text{if } C(i, i) \neq C'(i, j) \end{cases} \quad (12)$$

$$UACI = \frac{1}{M \times N} \left[\sum_{i,j} \frac{C(i, j) - C'(i, j)}{255} \right] \times 100\% \quad (13)$$

Where $C(i, j)$ and $C'(i, j)$ denote the encrypted frames before and after one pixel of the original frames is changed and the ciphered frame that is changed. Table 9 shows the average of these two measures applied to the test video base. From these results we can find that our algorithm is more robust against differential attack compared to OEEA and AES.

The EOEEA operates on the entire three components of the image where each one is treated separately. However, OEEA operates on all three components in one pass. From these facts and at the end of treatment, the formed set of the three components R, G and B will not change in the case of OEEA but it will be completely changed in the case of EOEEA. This means that the resistibility of EOEEA against a differential attack is better than OEEA. However, the resistibility of these two algorithms is better than that of AES which is a block cipher algorithm.

Table 9. NPCR and UACI of encrypted videos (%).

Video	Algorithm	AES		OEEA		EOEEA	
		NPCR	UACI	NPCR	UACI	NPCR	UACI
Intelligent room (320x240)		91.12	30.2341	94.15	28.3019	99.12	27.4510
Laboratory (320x240)		87.10	29.4547	95.46	28.0023	97.52	26.9870
Hall way (320x240)		89.03	31.8452	96.78	29.3106	98.99	28.1098
Hall (176x144)		90.02	30.4518	93.21	28.9078	96.32	26.9072
Bootstrap (160x120)		92.01	30.3821	93.48	29.0643	96.71	27.5903
Shopping mall (320x256)		90.08	32.9840	96.09	30.0847	98.23	28.9614
Hall monitor (352x288)		89.90	29.3095	98.45	28.5401	99.04	26.8147

Force brute attack Brute force attack [43] is an attack used to break the key encryption systems by performing an exhaustive search for all possibilities of security key. Systems that have small key sizes are vulnerable to this attack as AES (key length is 192 or 256 bits). Our system generates three keys of 256 elements from the three RGB components encrypted. The final key of EOEEA algorithm is the concatenation of these three keys which gives a final key size of 768 numbers. So, it is 6144 bit size for images smaller than 255 pixels. Thus, the proposed algorithm penalizes any exhaustive attack.

Analysis of the key space The key space should be large enough to resist against brute force attack that is shown in the previous section. Thus, the encryption key of the system EOEEA changes from one image to another. In addition, the successive encryption of the same image gives a different set of pictures, so different keys are generated every time you encrypt the original image.

5 Conclusion

In this paper, we proposed a new partial video encryption system in order to protect ROI privacy in video surveillance applications. For ROI detecting, we proposed an improvement for GMM to eliminate the local variations and illumination changes; where we have used segmentation image algorithm to have homogeneous zones and each area have a supervisor which is a thread that can calculate the histogram in order to detect changes. The encryption of ROI is performed by an enhanced evolutionary encryption algorithm which is based on

genetic algorithms, exploiting the representation of the RGB color space to be treated in three parallel independent threads. We demonstrated through performance evaluation with many video in different conditions that the proposed scheme is able to effectively detect and protect the privacy of public. The experimental results showed that the proposed system has a number of satisfied constraints and a good strength such as: a good detection rate with a low false alarm rate, a reduced computational time, and high security level and does not affect the compression ratio greatly. We aim in the future to improve the ROI detection method in order to provide the highest level of the individuals' privacy protection in complex background environment.

References

1. Abomhara, M., Zakaria, O., Khalifa, O.O., Zaidan, A., Zaidan, B.: Enhancing selective encryption for h. 264/avcusing advanced encryption standard. *International Journal of Computer and Electrical Engineering* **2**(2), 223 (2010)
2. Beniani, R., Faraoun, K.M.: A mixed chaotic-cellular automata based encryption scheme for compressed jpeg images. *J. Multim. Process. Technol.* **9**(3), 88–101 (2018)
3. Boulton, T.E.: Pico: Privacy through invertible cryptographic obscuration. In: *Computer Vision for Interactive and Intelligent Environment (CVIIE'05)*. pp. 27–38. IEEE (2005)
4. Bouwmans, T.: Recent advanced statistical background modeling for foreground detection—a systematic survey. *Recent Patents on Computer Science* **4**(3), 147–176 (2011)
5. Brahim, F., Hamid, S., Herman, A.: A new approach for the extraction of moving objects. In: *Modeling Approaches and Algorithms for Advanced Computer Applications, Studies in Computational Intelligence*, vol. 488, pp. 27–36. Springer, Cham (2013)
6. Charoenpong, T., Supasuteekul, A., Nuthong, C.: Adaptive background modeling from an image sequence by using k-means clustering. In: *ECTI-CON2010: The 2010 ECTI International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology*. pp. 880–883. IEEE (2010)
7. Chuan-xu, W., Zuo-yong, L.: Face detection based on skin gaussian model and kl transform. In: *2008 Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing*. pp. 522–525. IEEE (2008)
8. Cui, W., Guan, Z., Zhang, Z.: An improved region growing algorithm for image segmentation. In: *2008 International Conference on Computer Science and Software Engineering*. vol. 6, pp. 93–96. IEEE (2008)
9. Daor, J., Daemen, J., Rijmen, V.: Aes proposal: Rijndael (1999)
10. Davis, L.: Applying adaptive algorithms to epistatic domains. In: *IJCAI*. vol. 85, pp. 162–164 (1985)
11. Dufaux, F., Ebrahimi, T.: Scrambling for privacy protection in video surveillance systems. *IEEE Transactions on Circuits and Systems for Video Technology* **18**(8), 1168–1174 (2008)
12. El-said, S.A., Hussein, K.F., Fouad, M.M.: Securing multimedia transmission using optimized multiple huffman tables technique. *International Journal of signal Processing, image processing and pattern recognition* **4**(1), 48–64 (2011)

13. Farou, B., Kouahla, M.N., Seridi, H., Akdag, H.: Efficient local monitoring approach for the task of background subtraction. *Engineering Applications of Artificial Intelligence* **64**, 1–12 (2017)
14. Farou, B., Rouabhia, H., Seridi, H., Akdag, H.: Novel approach for detection and removal of moving cast shadows based on rgb, hsv and yuv color spaces. *Computing and Informatics* **36**(4), 837–856 (2017)
15. FAROU, B., SERIDI, H., AKDAG, H.: Using gaussian mixture models and hsv color space for background subtraction. In: *CONTROL ENGINEERING TECHNOLOGIES CONFERENCE*. p. 135 (2013)
16. Farou, B., Seridi, H., Akdag, H.: Improved parameters updating algorithm for the detection of moving objects. In: *IFIP International Conference on Computer Science and its Applications*. pp. 527–537. Springer (2015)
17. Farou, B., Seridi, H., Akdag, H.: Improved gaussian mixture model with background spotter for the extraction of moving objects. *Int. Arab J. Inf. Technol.* **13**(6A), 807–816 (2016)
18. Fazli, S., Pour, H.M., Bouzari, H.: Multiple object tracking using improved gmm-based motion segmentation. In: *2009 6th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology*. vol. 2, pp. 1130–1133. IEEE (2009)
19. Grefenstette, J.J.: Optimization of control parameters for genetic algorithms. *IEEE Transactions on systems, man, and cybernetics* **16**(1), 122–128 (1986)
20. Guo, J., Xu, J.y., Bao, J.l.: Region of interest based selective encryption scheme for privacy protection in h. 264 video. *Journal of Shanghai Jiaotong University (Science)* **19**(4), 385–391 (2014)
21. Hong, K., Jung, K.: Partial encryption of digital contents using face detection algorithm. In: *Pacific Rim International Conference on Artificial Intelligence*. pp. 632–640. Springer (2006)
22. Hsu, R.L., Abdel-Mottaleb, M., Jain, A.K.: Face detection in color images. *IEEE transactions on pattern analysis and machine intelligence* **24**(5), 696–706 (2002)
23. Khalid, M.S., Ilyas, M.U., Sarfaraz, M.S., Ajaz, M.A.: Bhattacharyya coefficient in correlation of gray-scale objects. *Journal of Multimedia* **1**(1), 56–61 (2006)
24. Li, H., Gu, Z., Deng, L., Han, Y., Yang, C., Tian, Z.: A fine-grained video encryption service based on the cloud-fog-local architecture for public and private videos. *Sensors* **19**(24), 5366 (2019)
25. Li, L., Huang, W., Gu, I.Y., Tian, Q.: Foreground object detection from videos containing complex background. In: *Proceedings of the eleventh ACM international conference on Multimedia*. pp. 2–10 (2003)
26. Li, L., Huang, W., Gu, I.Y.H., Tian, Q.: Statistical modeling of complex backgrounds for foreground object detection. *IEEE Transactions on Image Processing* **13**(11), 1459–1472 (2004)
27. Li, S.Y., Benalcazar Hernandez, M.A., Tam, L.M., Chen, C.S.: A cloud image data protection algorithm with multilevel encryption scheme and automated-selection mechanism. *Applied Sciences* **9**(23), 5146 (2019)
28. Li, S.: Encryption-friendly multimedia coding and communications: Is it necessary and possible? *IEEE Multimedia Communications Technical Committee E-Letters* **4**(1), 15–18 (2009)
29. Lian, S., Zhang, Y., Park, J.H., Kitsos, P.: Secure multimedia communication. *Security and Communication Networks* **1**(6), 437–440 (2008)
30. Liu, H., Wang, X., et al.: Image encryption using dna complementary rule and chaotic maps. *Applied Soft Computing* **12**(5), 1457–1466 (2012)

31. Martel-Brisson, N., Zaccarin, A.: Learning and removing cast shadows through a multidistribution approach. *IEEE Transactions on Pattern Analysis and Machine Intelligence* **29**(7), 1133–1146 (2007)
32. Meibing, Q., Xiaorui, C., Jianguo, J., Shu, Z.: Face protection of h. 264 video based on detecting and tracking. In: 2007 8th International Conference on Electronic Measurement and Instruments. pp. 2–172. IEEE (2007)
33. Nebili, W., Farou, B., Seridi, H.: Using resources competition and memory cell development to select the best gmm for background subtraction. *International Journal of Strategic Information Technology and Applications (IJSITA)* **10**(2), 21–43 (2019)
34. Nebili, W., Farou, B., Seridi, H.: Background subtraction using artificial immune recognition system and single gaussian (airs-sg). *Multimedia Tools and Applications* **79**(35), 26099–26121 (2020)
35. Pak, C., An, K., Jang, P., Kim, J., Kim, S.: A novel bit-level color image encryption using improved 1d chaotic map. *Multimedia Tools and Applications* **78**(9), 12027–12042 (2019)
36. Peng, F., Zhu, X.w., Long, M.: An roi privacy protection scheme for h. 264 video based on fmo and chaos. *IEEE transactions on information forensics and security* **8**(10), 1688–1699 (2013)
37. Prati, A., Mikic, I., Trivedi, M.M., Cucchiara, R.: Detecting moving shadows: algorithms and evaluation. *IEEE transactions on pattern analysis and machine intelligence* **25**(7), 918–923 (2003)
38. Quintiliano, P., Guadagnin, R., Santa-Rosa, A.: Practical procedures to improve face recognition based on eigenfaces and principal component analysis. *PATTERN RECOGNITION AND IMAGE ANALYSIS C/C OF RASPOZNAVANIYE OBRAZOV I ANALIZ IZOBRAZHENII* **11**(2), 372–375 (2001)
39. Rahman, S.M.M., Hossain, M.A., Mouftah, H., El Saddik, A., Okamoto, E.: Chaos-cryptography based privacy preservation technique for video surveillance. *Multimedia systems* **18**(2), 145–155 (2012)
40. Rajpoot, Q.M., Jensen, C.D.: and privacy in video : requirements and challenges. In: *IFIP International Information Security Conference*. pp. 169–184. Springer (2014)
41. Rodrigues, J.M., Puech, W., Meuel, P., Bajard, J.C., Chaumont, M.: Face protection by fast selective encryption in a video (2006)
42. Rouabhia, H.E., Farou, B., Kouahla, Z.E., Seridi, H., Akdag, H.: Cooperative processing based on posture change detection and trajectory estimation for unknown multi-object tracking. *International Journal of Systems Science* **50**(13), 2539–2551 (2019)
43. Schneier, B.: *Applied cryptography protocols, algorithms and source code in c* (1995)
44. Senior, A.W., Pankanti, S.: Privacy protection and face recognition. In: *Handbook-of-face-recognition*, pp. 671–691. Springer (2011)
45. Shahid, Z., Chaumont, M., Puech, W.: Fast protection of h. 264/avc by selective encryption of cavlc and cabac for i and p frames. *IEEE Transactions on Circuits and Systems for Video Technology* **21**(5), 565–576 (2011)
46. Shahid, Z., Puech, W.: Visual protection of hevc video by selective encryption of cabac binstrings. *IEEE transactions on multimedia* **16**(1), 24–36 (2013)
47. Shi, C., Wang, S.Y., Bhargava, B.: Mpeg video encryption in real-time using secret key cryptography. In: *in Proc. Int. Conf. Parallel and Distributed Processing Techniques and Applications*. Citeseer (1999)

48. Shiguo, L.: *Multimedia Content Encryption: Algorithms and Application*. Auerbach Publications, CRC Press, 1 edn. (2008)
49. Souici, I., Seridi, H.: Une mthode rapide et efficace pour le cryptage volutionnaire d'images. In: *Colloque sur l'Optimisation et les Systmes d'Information COSI'2011*. COSI (01)
50. Souici, I., Seridi, H., Akdag, H.: Images encryption by the use of evolutionary algorithms. *Analog Integrated Circuits and Signal Processing* **69**(1), 49–58 (2011)
51. Stauffer, C., Grimson, W.E.L.: Adaptive background mixture models for real-time tracking. In: *Proceedings. 1999 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (Cat. No PR00149)*. vol. 2, pp. 246–252. IEEE (1999)
52. Stinson, D., Vaudenay, S., Avoine, G., Junod, P.: *Cryptographie-Théorie et pratique/2ème édition*, vol. 1. vuibert, 2 edn. (2003)
53. Talhaoui, M.Z., Wang, X., Talhaoui, A.: A new one-dimensional chaotic map and its application in a novel permutation-less image encryption scheme. *The Visual Computer* pp. 1–12 (2020)
54. Tang, L.: Methods for encrypting and decrypting mpeg video data efficiently. In: *Proceedings of the fourth ACM international conference on Multimedia*. pp. 219–229 (1997)
55. Wang, X., Guan, N., Zhao, H., Wang, S., Zhang, Y.: A new image encryption scheme based on coupling map lattices with mixed multi-chaos. *Scientific reports* **10**(1), 1–15 (2020)
56. Wang, X., Zhao, H., Hou, Y., Luo, C., Zhang, Y., Wang, C.: Chaotic image encryption algorithm based on pseudo-random bit sequence and dna plane. *Modern Physics Letters B* **33**(22), 1950263 (2019)
57. Wu, C.P., Kuo, C.C.: Design of integrated multimedia compression and encryption systems. *IEEE Transactions on Multimedia* **7**(5), 828–839 (2005)
58. Yaco, B.Z., Rahma, A.S.: Real-time partial encryption of oigital video using symmetric dynamic dual keys algorithm (sdd). *Engineering and Technology Journal* **30**(5), 710–728 (2012)
59. Zeng, W., Lei, S.: Efficient frequency domain selective scrambling of digital video. *IEEE Transactions on Multimedia* **5**(1), 118–129 (2003)
60. Zhang, P., Thomas, T., Emmanuel, S.: Privacy enabled video surveillance using a two state markov tracking algorithm. *Multimedia systems* **18**(2), 175–199 (2012)
61. Zhang, Z., Yu, S.: On the security of a latin-bit cube-based image chaotic encryption algorithm. *Entropy* **21**(9), 888 (2019)