ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Highly Secure Scalable Compression of Encrypted Images using Chaos and AES Algorithms

Syamily S Kumar[1], Aida Sebastian[2]

PG Student, Department of ECE, College of Engineering Kallooppara, Thiruvalla, India [1]

Assistant Professor, Department of ECE, College of Engineering Kallooppara, Thiruvalla, India[2]

ABSTRACT: In this paper a highly efficient image encryption-then compression (ETC) system is introduced. For high level security the images have to be encrypted before compression. Encryption is done by using AES method by simple XORing operation. In the encrypted domain suitable shuffling method is adopted to offer more security and avoid hacking of data. A scalable compression based approach is applied to shuffled images via context adaptive sampling. Compression achieved by Base layer and Enhancement layer bits. Extra samples in enhancement layer bit obtained by greedy strategy. The bit stream in the base layer is produced by coding a series of non overlapping patches of the uniformly down-sampled version of the encrypted image. At the decoder side, an iterative, multiscale technique is developed to reconstruct the image from all the available pixel samples. Image is reconstructed by Soft adaptive interpolation technique

KEYWORDS*:* Advanced Encryption Standard(AES),Shuffling method,Compression,Soft Adaptive Interpolation(SAI),Context adaptive sampling**,**

.

I. INTRODUCTION

Nowadays security of information is more and more important, when the data are transmitted over open network frequently. Cryptography plays an important role in data security for that image has to be encrypted before compression. Encryption is the process of translating plain text data (plaintext) into something that appears to be random and meaningless (cipher text), only the authorized person can see it. Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. In a cryptosystem, the data are to be first compressed and then encrypted. But in some cases the reverse ordering is used. This system offers more security and there is no compromise in compression efficiency.

In addition to security efficient utilization of channel is also needed for better bandwidth allocation and memory utilization. In encryption then compression system (ETC) channel utilization done by compression technique. Data compression or source coding is the process of encoding information using fewer bits. Here in this paper compression done in encrypted domain. The objective of image compression is to reduce redundancy and store or transmit data in efficient form. Consider the problem of transmitting redundant data over an insecure, bandwidth-constrained communications channel, it is desirable to both encrypt and compress the data. In this paper, our primary focus is on the design of a scalable compression of stream cipher encrypted images through context adaptive sampling for encrypted images, such that the end terminal can receive and recover the coded images at different resolution and quality levels. We first define a measure of secrecy based on the statistical correlation of the original source and the compressed, encrypted source. An iterative, multiscale technique is developed to reconstruct the image from all the available pixel samples. The goal of encryption then compression of stream cipher encrypted image is to achieve better security and confidentiality in addition to reduction of redundancy. But there are problem related to compression efficiency and security. In this study a novel technique used to overcome the difficulties. This method can be applied for various applications

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

II. RELATED WORK

Considerable research has been conducted to compress encrypted images. The standard way of providing security is by advance encryption standard(AES) or data encryption standard(DES),RC4[2].Liuet Al developed a lossless, progressive approach to compress stream cipher encrypted greyscale/colour images. Recently, Klinc et al. extended Johnson's framework to efficiently compress block cipher encrypted data. In addition to lossless compression of encrypted images, lossy compression, which offers higher compression ratios, was also investigated.
The conventional method to distribute redundant data over an insecure and bandwidth-limited channel is to perform compression before the encryption. However, recent work by Johnson et al. shows that it is possible to reverse the order, and neither the compression performance nor the security will be sacrificed under certain reasonable conditions. Johns net. Al proved that coding with side information principles could be used to compress stream cipher encrypted data, without hurting either the compression efficiency or the information theoretic security [3].D.Schonberg and S.Draper suggest 2-D source model and develop a scheme to compress encrypted images based on LDPC codes [5].

III. PROPOSED ALGORITHM

A. *Block diagram:*
For ensuring security encryption is done. In addition to encryption hacking can be avoided by bit shuffling in encrypted domain. The shuffled bit is sending to the communication channel here suitable processing take place. Channel utilization done by compression technique. In proposed system base and enhancement layer is used to compress the encrypted data.The bit stream in the base layer is produced by coding a series of non overlapping patches of the uniformly down-sampled version of the encrypted image. Extra samples are coded in enhancement layer.Thses two bits are sends to the receiver side. Where corresponding decryption and reconstruction of image taken place.

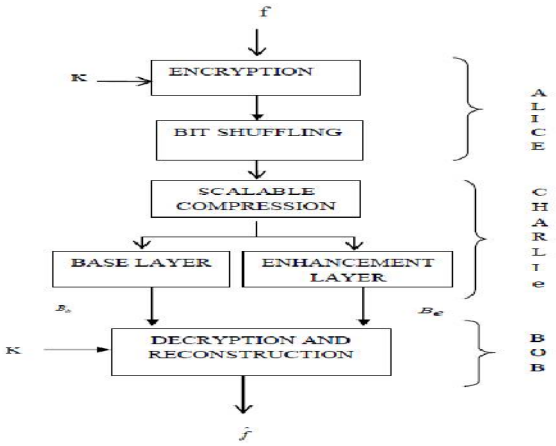

Fig1. Block Diagram of the proposed System

B. *Description of the Proposed Algorithm:*
The proposed method consists of Alice and Bob communication in presence of third party like Charlie. Alice wants to securely transmit information in presence of untrusted communication channel. As the content owner, Alice is always interested in protecting the privacy of the image data through encryption. Nevertheless, Alice has no incentive to compress her data, and hence, will not use her limited computational resources to run a compression algorithm before encrypting the data. This is especially true when Alice uses a resource-deprived mobile device developed.
In contrast, the channel provider Charlie has an overriding interest in compressing all the network traffic so as to maximize the network utilization. It is therefore much desired if the compression task can be delegated by Charlie, who typically has abundant computational resources. A big challenge within such Encryption-then-Compression (ETC) framework is that compression has to be conducted in the encrypted domain, as Charlie does not access to the secret key K.In contrast, the channel provider Charlie is always interested in compressing all the network traffic in a flexible and scalable way, such that the network utilization is maximized. Also, delivering the encrypted image in a scalable manner enables the end terminal to receive and decode the image at different resolution and quality levels. Note that the

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

compression task of Charlie has to be conducted over the encrypted domain, as he has no access to the secret key. This system includes, the details of the three key components in proposed ETC system, namely, image encryption conducted by Alice, image compression conducted by Charlie, and the sequential decryption and decompression conducted by Bob. Encryption refers to set of algorithms, which are used to convert the plain text to code or the unreadable form of text, and provides privacy. To decrypt the text the receiver uses the "key" for the encrypted text. It has been the old method of securing the data, which is very important for the military and the government operations. Now it has stepped into the civilian's day-to-day life too. The online transactions of banks, the data transfer via networks, exchange of vital personal information etc. that requires the application of encryption for security reasons.

IV.ENCRYPTION

Encryption is the process of encoding messages or information in such a way that only authorized parties can read it. The technique involves three different phases in the encryption process. The first phase is the image encryption where the image is split into blocks and these blocks are permutated. Further permutation is applied based on a random number to strengthen the encryption. The second phase is the key generation phase, where the values used in the encryption process are used to build a key. The third phase is the identification process which involves the numbering of the shares that are generated from the secret image. These shares and the key are then transferred to the receiver. The receiver takes the help of the key to construct the secret image in the decryption process. The technique proposed is a unique one from the others in a way that the key is generated with valid information about the values used in the encryption process. Most of the encryption processes first generate the key and then do the encryption process. This technique generates a relation between the encryption process and the key.

The current work focuses on designing a scalable compression scheme of stream cipher encrypted images, where encryption is carried out by applying a stream cipher in the standard format. Stream ciphers are an important class of encryption algorithms. They encrypt individual characters (usually binary digits) of a plaintext message one at a time, using an encryption transformation which varies with time. By contrast, block ciphers tend to simultaneously encrypt groups of characters of a plaintext message using a fixed encryption transformation. Stream ciphers are generally faster than block ciphers in hardware, and have less complex hardware circuitry. They are also more appropriate, and in some cases mandatory (e.g., in some telecommunications applications), when buffering is limited or when characters must be individually processed as they are received. Because they have limited or no error propagation, stream ciphers may also be advantageous in situations where transmission errors are highly probable. Stream ciphers can be either symmetric-key or public-key. In this project we focused on symmetric key stream cipher.

V. BIT SHUFFLING

In this approach we have proposed a new algorithm which utilizes the single map against the four maps used in earlier papers. We used Henon map and Lorentz map for pixel shuffling and measured correlation coefficient and key sensitivity for finding best suited map for this algorithm. The key space will become less with single map utilization and hence better suited for applications like wireless communication. At the same time it gives better secrecy and a key which is difficult to decipher by an unintended user.

Consider an image (Io) with dimension M×N×P, Where, P represents colour combination (3 for a colour image); M, N represents rows and column of intensity level. Separate R, G, B matrix of Image and convert each R, G, B matrix into single array (1×mn). For example, Lena image which is one of the common image used for image processing algorithms has a dimension of 225× 225 × 3 and after separation of R, G, B and converting it in to single array vectors, we get 3 vectors of dimension 1× 50625. For bit shuffling we first generate elements from chaos map equal to the dimension of 3×M×N matrix. In our example of Lena image 225×225×3=151875 elements are generated with Henon map. The Henon map [2] can be generated using the equation given below which is iterated for n=1 to 151875 times to generate the required elements.

$$x(n+1) = 1 - a * x(n)^{2+y(n)}; \; y(n+1) = b * x(n) \qquad (1)$$

We used the following values for the constants 'a' and 'b' to get a random sequence,
a=1.76, b=0.1and y (n) =1
The same procedure is repeated with Lorentz map. Following equations describes Lorentz map [2] ,

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

$$X(1) = s * y(i-1,2) - y(i-1,1));$$
$$X(2) = r * y(i-1,1) - y(i-1,2) - y(i-1,1) * y(i-1,3);$$
$$X(3) = y(i-1,1) * y(i-1,2) b * y(i-1,3)$$
$$y(1,:) = y(i-1,:) + b * X \quad (2)$$

For this map, we used the following values for the constants 's','y','h', 'b'and 'r' to get a random sequence. s=10, b=3, r=30, h=0.01 and y= [0.1, 0.1, 0.1].Now divide the generated elements into three blocks of each equal to M×N. Now sort the elements of each block in ascending or descending order and compare the misorder between the original and sorted elements of each block and tabulate the index change. We have got three series of index change values in according to three blocks.

VI.COMPRESSION

Compression is the art of reducing the number of bits or encoding information using fewer number of bits.The image compression algorithms is used to reduce the memory space or transmission time. In our work compression done by

- Base layer coding
- Enhancement layer coding

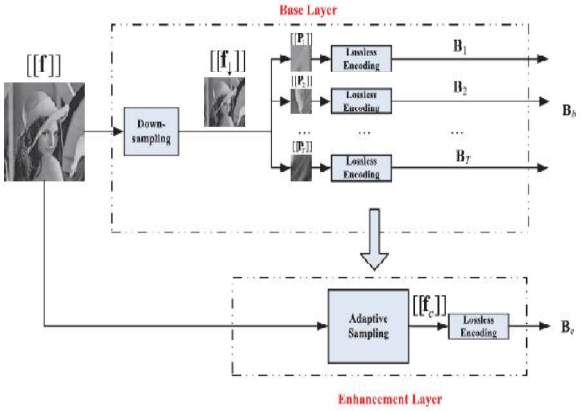

Fig 2 The proposed scalable image coding scheme

A. Base Layer Encoding

To generate the bit stream in the base layer, we first down-sample [[f]] into [[f↓]]. Here, we stick to conventional square pixel grid by uniform spatial down sampling of [[f]]. Out of practical considerations, we make a more compact representation of [[f]] by decimating every four rows and every four columns, namely, the resulting [[f↓]] is of size N/4×N/4. This simple down-sampling strategy can be readily implemented in the encrypted domain, as the spatial relationship among pixels keeps unchanged after encryption. Further, such down-sampling offers an important operational advantage: [[f↓]] still remains a uniform rectilinear grid of pixels making it readily compressible by any existing techniques for compressing encrypted images. Instead of coding [[f↓]] as a whole, we propose to partition it into a series of non-overlapping patches [[Pt]] of size M × M. Each [[Pt]] is then treated as a sub image, and coded individually into a binary bit stream But, by applying the lossless compression method. As the coding of each [[Pt]] is independent with that of the other patches. Base layer coding done by resolution progressive compression.The encoder starts by sending a downsampled version of the ciphertext.At the decoder, the corresponding low-resolution image is decoded and decrypted, from which a higher-resolution image is obtained by intraframe prediction. The predicted image, together with the secret encryption key, is used as the side information (SI) to decode the next resolution level. This process is iterated until the whole image is decoded.By doing so, the task of de-correlating the pixels, which is not possible for the encoder, is shifted to the decoder side. In addition, by having access to a lower-resolution image, the decoder is able to learn the local statistics, doing much better than "blind" decoding. Moreover, by avoiding exploiting the Markovian property in Slepian-Wolf decoding, the decoder's complexity significantly reduced.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

1 .Resolution Progressive Compression

The encoder gets the ciphertextY and decomposes it into four sub images, namely, the 00, 01, 10, and 11 sub-images. Each sub-image is a downsampled-by-two version of the encrypted image. The name of a sub-image denotes the horizontal and vertical offsets of the downsampling. The 00 sub-image is further downsampled to create multiple resolution levels. We use 00_n to represent the 00 sub-image in the n-th resolution level. The 00_n sub-image can be losslessly synthesized from the 00_{n+1}, 01_{n+1}, 10_{n+1} and 11_{n+1} sub-images. After the downsampling, each sub-image is encoded independently using Slepian-Wolf codes, and the resulting syndrome bits are transmitted from the lowest resolution to the highest. Decoding starts from the 00 sub-image of the lowest-resolution level, say, level N.

We suggest transmitting the uncompressed 00_N sub-image as the doped bits . Thus, the 00_N sub-image can be known by the decoder without ambiguity, and knowledge about the local statistics will be derived based on it. Next, other sub-images of the same resolution level are interpolated from the decrypted image. After the interpolation step SI of the plaintext is obtained and then generates the SI of the cipher text. This is a one-to-one mapping between the SI of the plain text and cipher text. From the SI, the conditional pdf of the original pixel values are calculated with the help of a channel estimation module. Then the SI estimated PDF and the key is passed to the decoder. The decoder decrypts the 01n, 10n, 11n and then 00n-1 can be synthesized. Repeat the process till the target is obtained. If the SI is a good approximation of the target image the pixels are conditionally independent to each other and there is no need of the Markovian property of SlepianWolf decoding. The encoder accompanies a feedback channel and this channel reports how many bits are transmitted for each subimage.This increase the transmission delay. But this is reasonable.

C. *Enhancement Layer*

In this subsection discuss the strategy of selecting pixel samples to be coded in the enhancement layer. Let $\tilde{h} = (\tilde{h}_1, \tilde{h}_2, ..., \tilde{h}_T)'$, where $\tilde{h}_i$ denotes the **LCI** value of the *i*th 4*M* × 4*M* sized patch of the encrypted image and *T* is given by,

$$T = \frac{N^2}{16M^2} \tag{3}$$

We also define the sample selection vector $n = (n_1, n_2, ...n_T)'$, where $n_i \times s$ is the number of samples selected from the *i*th 4*M* × 4*M* patch. Let us assume that totally there are $F \times s$ samples to be coded in the enhancement layer, where *F* is a non-negative integer controlling the overall coding rate. A natural criterion for selecting the pixel samples to be coded in the enhancement layer is to minimize the total reconstruction error. Therefore, the determination of all n_i's can be mathematically formulated as the following optimization problem

$$\min_{n} \sum_{i=1}^{T} e(n) \tag{4}$$

where $e(n_i)$ denotes the reconstruction distortion when $n_i \times s$ additional pixel samples are provided. Noticing the fact that all n_i s are integers, the above optimization problem essentially belongs to the category of integer programming problems. Which are unfortunately NP-hard. In other words, no polynomial-time algorithm exists for solving (10).To reduce the computational burden while still achieving reasonably good performance, we develop a greedy algorithm consisting of *F* stages. In each stage, *s* samples will be allocated, aiming at minimizing the induced reconstruction distortion at that particular stage. As will become clear shortly, the complexity of our proposed greedy heuristic is of order *(F × T)*, where *T* given in (3) is the number of 4*M* × 4*M*sized patch.

As the vector $\tilde{h} = (\tilde{h}_1, \tilde{h}_2, ..., \tilde{h}_T)'$ and the initial **E** together with its updating rule are completely transparent to the decoder, the same operations can be performed by the decoder to determine the locations of the samples upon decoding the bit steam received from the enhancement layer. As we need to perform *T* times of comparison at each stage, and there are totally *F* stages, the complexity of the above greedy algorithm is of order *O(F×T)*. In terms of the overall

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

complexity of the enhancement layer, we observe that it is primarily dominated by the actual coding of those selected pixel samples, rather than the above greedy selection process. Hence, the complexity of the enhancement layer almost linearly increases with the number of pixel samples coded.

VII. IMAGE RECONSTRUCTION

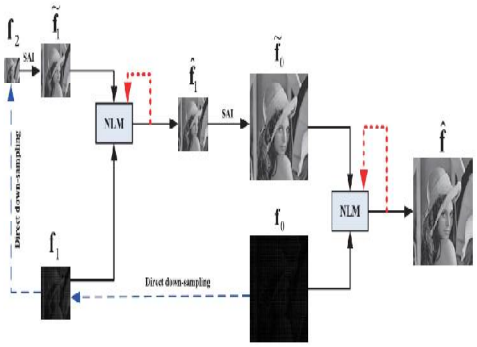

Fig 4 schematic representation of image reconstruction

Upon receiving the bit stream Bb from the base layer, the decoding algorithm of [7] can be applied to get [[f↓]]. As the uniform down-sampling rule is public and the encryption of each bit is independent with that of the others, the encoder and the decoder can be straight forwardly synchronized. Hence, [[f↓]] can be appropriately decrypted into f↓ by XORing with the corresponding key stream. In the case that the enhancement layer is not available, f↓ can be directly up-converted to $\hat{f}_b$, which is of the same size as the original image f, using the method to be presented below. In some application scenarios, $\hat{f}_b$ can be utilized as the preview version for customers. When the bit stream of the enhancement layer arrives, the decoding algorithm of [7] can be similarly employed to obtain [[fe]], where the base layer reconstruction $\hat{f}_b$ serves as the side information. As the encoder and the decoder are perfectly synchronized, the key stream can be appropriately extracted to decrypt [[fe]] into fe. With f↓ and fe, the decoder aims to go beyond and collaboratively re-estimate the original image.

To this end, we propose an iterative, multi-scale technique to reconstruct the original image, as depicted in Fig. 5. Let f0 be the image containing all the available samples from f↓ and fe, while the vacant locations are padded with 0's. In our proposed multiscale framework, f0 is successively down-sampled twice by a factor of 2 respectively to form a pyramid: f1 and f2, by duplicating the corresponding pixels from the existing high resolution images. The image reconstruction starts from the lowest level 2. We first up-convert f2 to a higher level $\tilde{f}_1$ via a parametric-model based interpolation method. Due to the excellent interpolation performance and modest computational complexity, the soft-decision adaptive interpolation (SAI) based on 2D-piecewise autoregressive (2D-PAR) model is adopted.

VIII. SIMULATION RESULTS

The proposed method has been applied on various images and successful results based on the quality of the reconstructed image. Quality of the reconstructed image is defined by the robustness, amount of noise and so on. Also, it is resistant to different security breaches that may affect the authenticity of the information. The image used in the experiment is of the bmp, jpg format And the size is limited to 512×512 .The AES algorithm allows a key of length 128bit,192bit and256. Here we use key of 128 bit length . In our experiment we have both the original and the reconstructed images to measure the quality. Here PSNR,SSIM index,CR and Bit Error Rate between the two images are taken and it is shown in the table below .

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

(a) (b)

Fig 5.visual comparison of Lena image (a) Original; (b) Reconstructed image

Visually the reconstructed and original image are identical. So the recommended method is can be used for practical purpose with less distortion.

Images	PSNR	BER	MSER	CR
Lena	8.9316	1	8.3161e+03	59.5782
Barbara	8.6325	1	8.9090e+03	59.5782
mandrill	9.6065	1	7.1192e+03	59.5782
Baboon	8.4389	0.9958	6.9732+03	59.5782
pepper	8.6014	1	7.6754e+03	59.5782
Boat	9.0912	0.9961	8.8754e+03	59.5782
Harbor	9.5674	1	8.3081e+03	59.5782

Table 1.Performance evaluation with AES encryption only

Table 1 shows the performance evaluation using AES encryption only.AES is Advanced Encryption Standard.It provide security. From the table it is clear that the method is best suited for practical purpose. Peak signal to noise ratio, bit error rate, mean square error and compression ratios are given

Images	PSNR	BER	MSER	CR
Lena	8.9316	1	8.3161e+03	59.5782
Barbara	8.6325	1	8.9090e+03	59.5782
mandrill	9.6065	1	7.1192e+03	59.5782
Baboon	8.4389	0.9958	6.9732+03	59.5782
pepper	8.6014	1	7.6754e+03	59.5782
Boat	9.0912	0.9961	8.8754e+03	59.5782
Harbor	9.5674	1	8.3081e+03	59.5782

Table2.Perfomance evaluation

Table 2 shows the performance evaluation of combined effect of chaos and AES technique. After encryption using AES bits are shuffled using chaos algorithm. This is actually an encryption process. So the system secured more. Hacking of datas are now difficult. From these tables it is clear that the modification algorithm doesn't alter the performance also improves security. The algorithm used for modification is better and recommended.

IX. CONCLUSION AND FUTURE WORK

In this paper, we design a novel scalable image coding scheme for stream cipher encrypted images. The base layer compresses a series of non-overlapping patches of the uniformly down-sampled version of the encrypted image. Based on the free side information offered by base layer coding, the enhancement layer strategically selects additional pixel samples to code. n. In base layer, a series of patches of downsampled image is compressed and the enhancement layer selects the additional pixel samples to be compressed. Then the image is reconstructed by the interpolation method. The

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

decoder then applies an iterative, multiscale technique to reconstruct the image from all the available samples. Experimental results verify the superior coding performance of our proposed work.

ACKNOWLEDGMENT

The authors would like to thank all the staffs of Department of ECE, college of engineering, kallooppara for their constant encouragement and support.

REFERENCES

1. Jianto Zhou,Oscar C Au,Guangtao Zhai,Yuan Yan tang and Zianing Liu" compression of stream cipher encrypted imges through context adaptive sampling"IEEE Trans.inf.forensic security,vol.9,no.11Nov 2014
2 A. A. Kumar and A. Makur,"Lossy compression of encrypted image by compressive sensing technique," in Proc. IEEE Region 10th Conf., Jan. 2009, pp. 1–6.
3. X Zhang, Y. Ren, G. Feng, and Z. Qian, "Compressing encrypted image using compressive sensing," in Proc. 7th IEEE Int. Conf. IIH-MSP, Oct. 2011, pp. 222–2225.
4. X. Zhang, G. Feng, Y. Ren, and Z. Qian, "Scalable coding of encrypted images," IEEE Trans. Image Process., vol. 21, no. 6, pp. 3108–3114, JuX. Zhang, "Lossy compression and iterative reconstruction for encrypted image," IEEE Trans. Inf. Forensics Security, vol. 6, no. 1, pp. 53–58, Mar. 2011.
5. X. Zhang, G. Sun, L. Shen, and C. Qin, "Compression of encrypted images with multi-layer decomposition," Multimedia Tools Appl., vol. 72, no. 1, pp. 489–502, Feb. 2013.
6. X. Kang, A. Peng, X. Xu, and X. Cao, "Performing scalable lossy compression on pixel encrypted images," EURASIP J. Image Video Process., vol. 2013, no. 32, pp. 1–6, May 2013

BIOGRAPHY

Syamily S Kumar is currently pursuing M-TECH in electronics with specialisation in signal processing, college of Engineering, kallooppara.She received her B-Tech(ECE) from the Musaliar College of Engineering and Technology, Pathanamthitta in 2014.Her areas of interest are Digital communication, Digital image processing and embedded design.

Aida Sebastin is currently an Assistant Professor with the Department of Electronics and Communication, College of Engineering, Kallooppara. She received her masters in Electronics from St Michael's College Of Engineering And Technology, Madurai