HIGHLY SECURE SCALABLE COMPRESSION OF ENCRYPTED IMAGES

Maria Joseph[1], Tomson Devis[2]

[1] *M.Tech student, Department of Electronics & Communication Engg., St. Joseph's College of Engineering & Technology-Palai, Kerala, India,* ***hellomariajoseph@gmail.com***

[2] *Assistant Professor, Department of Electronics & Communication Engg., St. Joseph's College of Engineering & Technology-Palai, Kerala, India,* ***tomsondevis@yahoo.com***

Abstract

A highly secure scalable compression method for stream cipher encrypted images is described in this journal. The input image first undergoes encryption and then shuffling. This shuffling in the image pixels enhances the security. For shuffling, Henon map is used. There are two layers for the scalable compression namely base layer and enhancement layer. Base layer bits are produced by coding a series of non-overlapping patches of uniformly down sampled version of encrypted image. In the enhancement layer pixels are selected by random permutation and then coded. From all the available pixel samples an iterative multi scale technique is used to reconstruct the image and finally performs decryption. The proposed method has high security.

Key Words: *Encryption, Decryption, Shuffling, Scalable compression*

----------***----------

1. INTRODUCTION

The role of computers and networks has made considerable change in human life. So one of the important issues we should consider is that protecting our data from a third party. Most of the data that we send through our network is clear and it is easy for an unwanted person to capture it. Encryption is considered as the method of transforming the data into a secret code. To read an encrypted data there must access to the secret key so that we can decrypt it. Modern encryption algorithm uses a key to decrypt it.

Encryption is actually a technique used to convert the data into an unreadable format. Each encryption algorithm uses a set of strings called key. Larger the length of key greater is the security. This is because when length of the key increases the possible number of combinations increases and thus make a third party to difficult to decrypt. A system used for encrypting and decrypting data is called cryptosystems. These usually involve combining plain text with one or more strings called key and making cipher text. The security of cryptosystems lies in the security of a key rather than the secrecy of algorithm. A strong cryptosystems has a wide range of possible key combinations and it is not possible to try all these key pairs. At the same time a strong cryptosystems will produce random output to all statistical methods and will resist to all methods for breaking codes.

Consider redundant data is transmitting through an insecure bandwidth limited channel. The traditional way to transmit this is to first compress it and then encrypt the data. Compression itself means removing the redundant patterns. Compression also means that reducing the dimensions. After compression there will be fewer bits. But there will contain more information per bit.

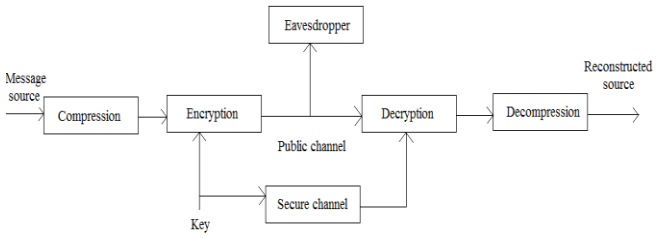

Fig -1: Traditional way of sending message

In this figure -1 an information source wants to send a message through a public channel. The traditional way to do this is to first compress and then encrypt. So the data is first compressed and then encryption takes place by using a secure key. At the receiver side, reverse process happens. i.e, first decryption and decompression happens. For decryption the same key used for encryption should be used. This is symmetric cryptography. That is, same key is used for both encryption and decryption. But there exist always an eavesdropper in the public channel for attacking the secure message.

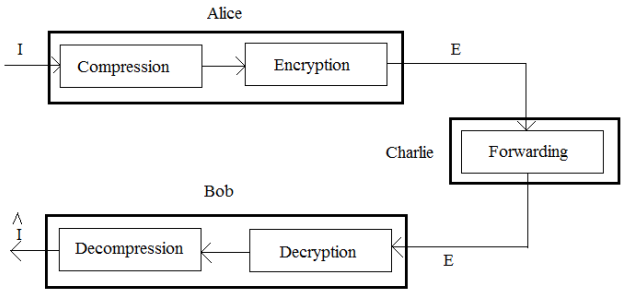

Fig -2: Compression Then Encryption (CTE) System

Consider a case in figure -2 in which Alice wants to send a message securely and efficiently to Bob through an untrusted channel provider Charlie. Conventionally this could be done as follows: Alice first compress the data into B and then encrypts into E using an encryption function E(K), where K is used as the secret key. The encrypted data E is then forwarded to Bob by Charlie, where Charlie is the network provider. Upon receiving E, Bob sequentially decode and decompress the message to retrieve the data I. This conventional system meets many requirements but even though in some situations we have to reverse the order of encryption and compression. Alice is always interested in securing her data. So she is only performing the encryption algorithm when she has limited number of computational resources. So in this case encryption is done by Alice at first and then Compression is done by Charlie. So this has led to Encryption Then Compression (ETC) System as in Figure -3. The main task here is that compression has to be carried out in the encryption domain as Charlie has no access to the secret key.

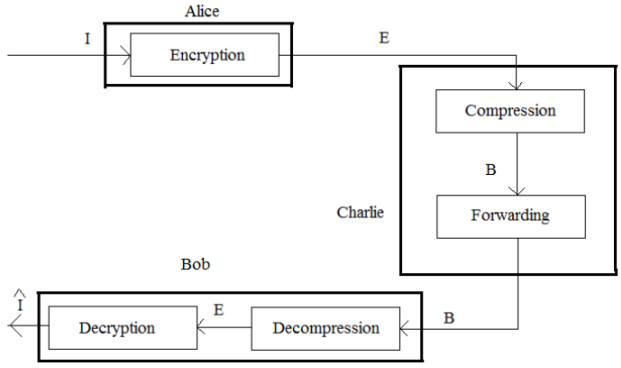

Fig -3: Encryption Then Compression (ETC) System

2. RELATED WORK

Jiantao et. al proposed a scalable compression method for stream cipher encrypted images [1]. They used standard stream cipher format. The bit stream in the base layer is produced by first down sampling the encrypted image and then a series of non-overlapping patches are formed which are uniform in nature. Johnson et. al examined the possibility of encrypting a data stream and compressing it without knowledge of key [2]. Using distributed source coding principles the encrypted data can be compressed because key will be available at the decoder. Schonberg et. al extended Johnson's work by considering information source with memory [3] [4]. Using minimal number of bits they transmitted encrypted source in this work. By applying LDPC codes in various bit planes and exploiting the intra/inter correlation Lazzeretti and Barni suggested method for lossless compression of gray/color images [5]. By using the principle of source coding with side information principle they recently demonstrated the possibility of lossless compression of encrypted images. Kumar and Makur applied Johnson et. al approach to the prediction error domain by using the iid property of prediction error sequences and achieved higher lossless compression performance for both gray scale and color images [6]. After the compression of gray scale and color images which is carried out in lossless domain only encryption is performed here. In addition to the lossless compression, lossy compression was also investigated which has higher compression ratios. Kumar and Makur proposed compressive sensing mechanism to compress encrypted images [7]. By using a modified pursuit algorithm the original image could be estimated from the compressed and encrypted data. Liu et. al proposed a lossless progressive compression technique for gray / color scale images [8]. Through Slepian Wolf coding lossless compression of encrypted images can be possible. Zhang designed an image encryption method by performing permutation operations in the pixel domain and showed that the resultant file can be compressed by discarding the fine and rough coefficients in the transform domain [9]. Here lossy compression of encrypted image is discussed with flexible compression ratio. Zhang et. al proposed a scalable lossy coding of encrypted images through a multi resolution construction. Here scalable coding of encrypted images is described [10]. Klinc et. al extended Johnson's work to efficiently compress block cipher encrypted data [11]. Here compression of block cipher is considered. Zhang et. al proposed a new technique for the compression of encrypted images through multi-layer decomposition [12]. This is lossy compression of encrypted gray images. Kang et. al proposed an interpolation based technique for decompressing and there compression is gained by down sampling and bit plane decomposition [13]. When more bit planes are transmitted higher quality of reconstructed image can be achieved. Zhang et. al proposes a method for compressing encrypted images in which the information owner Alice also generates some auxiliary information that can be used for compression and reconstruction [14].

3. PROPOSED METHODOLOGY

In this we consider conventional stream cipher which is applied in the standard format. That means cipher text is produced by bitwise XORing the plain text with the key stream. The scenario of scalable coding of encrypted image is shown in figure -4. This work proposes a novel scalable compression for shuffled encrypted images which has better security. The input image first undergoes encryption in the standard format (AES-CTR). For encryption we use AES-128. That means the secure key that we used here is of 128 bit length. After encryption, the encrypted image undergoes shuffling in order to increase the security. For shuffling we use Henon map. A Henon map has the most chaotic behavior. Here the Henon map takes a point and maps into another point by using these two equations.

$$X_{n+1} = 1-ax_n^2+y_n$$
$$Y_{n+1} = bx_n$$

The shuffled image undergoes scalable compression. There are two layers namely base layer and enhancement layer in the scalable compression. The base layer bits B_b and enhancement layer bits B_e are generated here. From those bits image is reconstructed and then undergoes rearrangement of pixels. After that, it is given to the decryption block where decryption is performed using the

same key stream. The scalable image encoding scheme is shown in figure -5. In order to generate base layer bits we first uniformly down sample the shuffled image which then undergoes wavelet decomposition. After that we divide the latter into different patches which must be a series of non-overlapping patches. Then we apply lossless encoding to each of the patch to produce the base layer bit stream. The final bit stream is generated by concatenating all the bits from patches. Extra bits for reconstruction other than base bits are produced by the enhancement layer. In this layer we select pixels by random permutation. The same procedure to generate base layer bits is adopted to this selected pixels and by applying lossless encoding enhancement bits is finally generated.

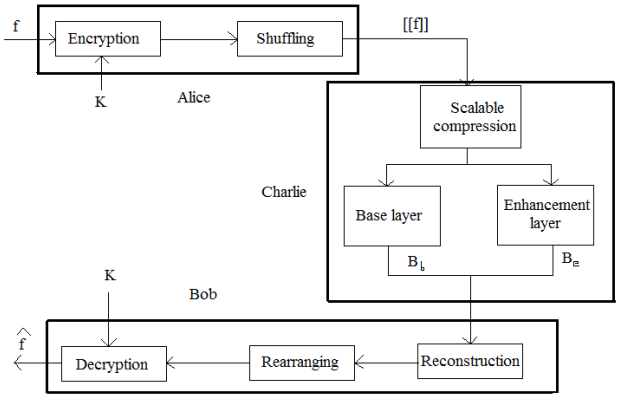

Fig -4: Scenario of scalable coding of encrypted images

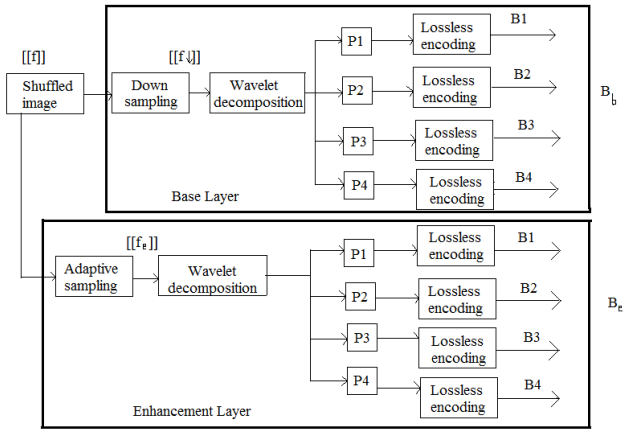

Fig -5: Scalable image coding scheme

At the receiver side reverse process happens. That is lossless decoding and wavelet reconstruction is done. And then the image is decoded. Then the pixels are rearranged by using sorting and Henon map. For final reconstruction of the image an iterative interpolation technique called Soft Adaptive Interpolation (SAI) is used. Finally the original image is retrieved by using decryption. Same 128 bit key that is used for encryption must be used for the proper decryption.

4. RESULTS AND DISCUSSION

The proposed method has been tested for different gray scale images. And it is possible to reconstruct the image with more security. It is implemented by using MATLAB 2012. For input image AES - CTR encryption is applied. Key used here is of 128 bit length. Figure -6 shows the input image which undergoes encryption and figure -7 shows the encrypted image. This encrypted image undergoes shuffling by using Henon map for better security. This is shown in figure -8. The shuffled image undergoes compression. This means that the shuffled image is the input to both the base and enhancement layer.

At the base layer the shuffled image is down sampled and then undergoes wavelet decomposition at level 3. This is shown in figure -9. After that it is divided into different patches and apply Slepian wolf encoding. The bits generated are shown in figure -10. Similarly enhancement layer bits are produced by applying wavelet decomposition and Slepian wolf encoding. This is shown in figure -11 and figure -12.

At the receiver side reverse process happens and the image is decoded. It is shown in figure -13. Rearrangement of pixels is then done. After that image is reconstructed by using Soft decision Adaptive Interpolation (SAI). This is shown in figure -14. Finally, decryption is performed and image is decrypted. It is shown in figure -15.

Fig -6: Input image

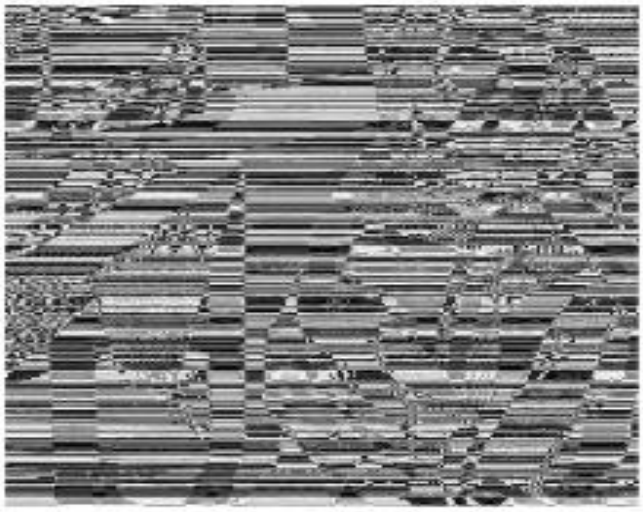

Fig -7: Encrypted image

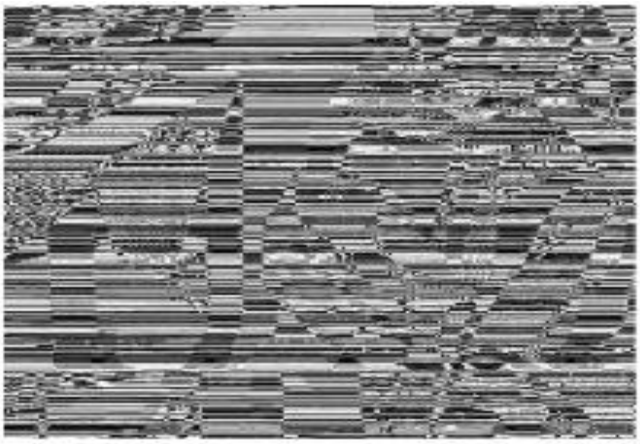

Fig -8: Shuffled image

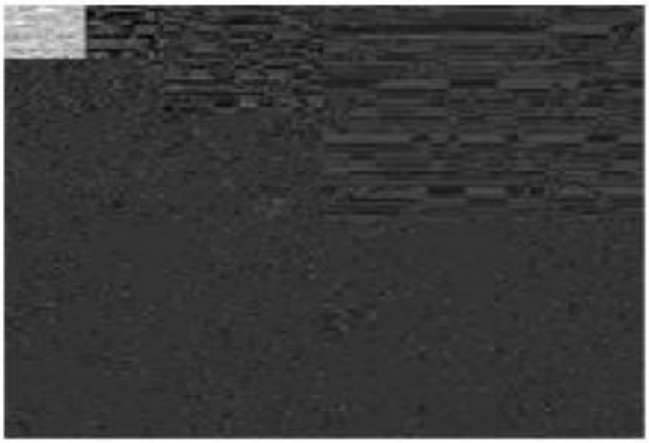

Fig -9: Wavelet decomposition at level 3 (base layer)

```
****************************************
Number of base layer encoded bits-:16285
Total number of bits in image-:524288
****************************************
```

Fig -10: Base layer bits

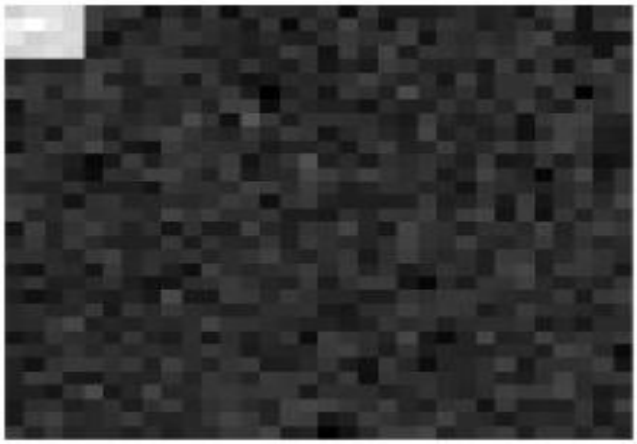

Fig -11: Wavelet decomposition (Enhancement layer)

```
************************************************************
Number of Enhancement layer encoded bits-:926
Total number of bits in image-:524288
************************************************************
```

Fig -12: Enhancement layer bits

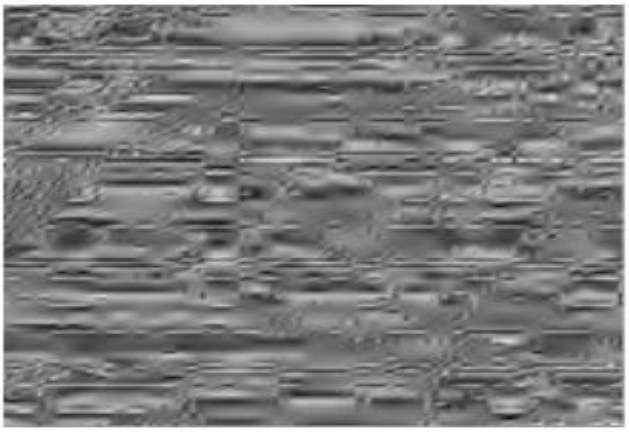

Fig -13: Decoded image

Fig -14: Reconstructed image

Fig -15: Decrypted image

5. CONCLUSION

This work proposes a highly secure scalable compression of stream cipher encrypted images. Security is achieved by shuffling the encrypted image by Henon map. Henon map has the highly chaotic behavior and pixel position will be mapped to a new position. The value of the pixel remains same here. The entire pixels will be shuffled and thus an eavesdropper cannot able to identify the original data. From the base layer and enhancement layer bits the decoder applies an iterative multi scale technique to reconstruct the

image. It has been tested on a large database and realized that the proposed method has high security.

REFERENCES

[1]. Jiantao Zhou, Oscar C. Au, Guangtao Zhai, Yuan Yan Tang and Xianming Liu, "Scalable compression of stream cipher encrypted images through context adaptive sampling", *IEEE transactions on Information Forensics and Security,* Vol. 9, No. 11, November 2014.

[2]. M. Johnson, P. Ishwar, V. Prabhakaran, D. Schonberg and K. Ramachandran, "On compressing encrypted data", *IEEE Trans. Signal Process.*,Vol. 52, No. 10, Oct 2004.

[3]. D. Schonberg, S. C. Draper and K. Ramachandran, "On blind compression of encrypted correlated data approaching the source entropy rate", *in Proc.43rd Annu. Allerton Conf. Commun., Control, Comput.,* 2005.

[4]. D. Schonberg, S. Draper and K. Ramachandran, "On compression of encrypted images", *in Proc. IEEE Int. Conf. Image Process.,* Oct. 2006.

[5]. R. Lazzeretti and M. Barni, "Lossless compression of encrypted grey level and color images", *in Proc. 16th Eur. Signal Process. Conf. (EUSIPCO),* 2008.

[6]. Kumar and A. Makur, "Distributed source coding based encryption and lossless compression of gray scale and color images", *in Proc. 10th Workshop MMSP,* Oct. 2008.

[7]. A Kumar and A. Makur, "Lossy compression of encrypted image by compressive sensing technique", *in Proc. IEEE Region 10th Conf.,* Jan. 2009.

[8]. W. Liu, W. Zeng, L. Dong and Q. Yao, "Efficient compression of encrypted grayscale images", *IEEE Tans. Image Process.,* Vol. 19, No. 4, Apr. 2010.

[9]. 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.

[10]. X. Zhang, G. Feng, Y. Ren and Z. Qian , "Scalable coding of encrypted images", *IEEE Trans. Image Process.,* Vol. 21, No.6, Jun. 2012.

[11]. D. Klinc, C. Hazay, A. Jagmohan, H. Krawczyk and T. Rabin, "On compression of data encrypted with block ciphers" *IEEE Trans. Inf. Theory,* Vol. 58, No. 11, Nov. 2012.

[12]. X. Zhang, G. Sun, L. Shen and C. Qin, "Compression of encrypted images with multi-layer decomposition", *Multimedia Tools Appl.,* Vol. 72, No. 1, Feb. 2013.

[13]. 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, May 2013.

[14]. X. Zhang, Y. Ren, L. Shen, Z. Qian and G. Freng, "Compressing encrypted images with auxiliary information", *IEEE Trans. Multimedia* Vol. 16, No. 5, Aug. 2014.