An Image Based Encryption Algorithm for Multimedia Applications

A. Mohanarathinam, S.Kamalraj, Prakash NB, Hemalakshmi GR, G.K.D.Prasanna Venkatesan

Abstract*: Multimedia is the most popular domain in recent era, where it handles distinct information such as text, image, music, video and etc. The security and channel capacity are the challenging parameters in real time multimedia applications. In this research work, an image based double encryption scheme has proposed along with DCT compression technique. The input image is encrypted by Chaotic Baker map and Advanced Encryption Standard (AES) algorithms. The encrypted image is compressed by DCT compression technique. The PSNR and MSE of proposed double encryption method attains 77.1617 and 0.0013 respectively. The experimental results are compared with the individual encryption methods shows that the performance of Double encryption is superior to the other existing methods.

***Keywords*: DCT compression, Advanced Encryption Standard, Chaotic-Baker Map, PSNR and MSE.**

I. INTRODUCTION

Compressing encrypted interactive media is an enhanced modernism planned towards diminishing the data computation of text signals without recognition plain-content setting [1-4]. In certain case the proprietor encodes the data for security insurance. In the wake of getting the compacted encoded data, an authorized client holding secret key can get back the original content. The aim is to effectively group the information and to make progress the information from the compressed data. Various handy plans utilizing Slepian-Wolf coding was implemented. For instance, the first parallel picture might be encoded by including a pseudorandom string, and the scrambled information packed as the disorders of low-density parity channel (LDPC) codes [2]. Compression of encrypted data for memory less and shrouded Markov sources utilizing LDPC codes [5], and compressive force for encoded dim and shading images utilizing LDPC codes in different piece planes [6] can be figured it out. Encryption is performed on expectation blunders [7] rather on plane pixels, and LDPC codes are used to set text writings. The text content is flawlessly decoded by neighborhood insights got from a low-goals rendition [8].

A lossless compression [9] for text writings programmed by AES and cipher-block chaining mode is created. Subsequent to delivering the figure content pictures by pixel-change, the scrambled information are packed by disposing of the unnecessarily unpleasant and fine data of coefficients produced from symmetrical change. At the recipient side, the disposed of harsh data of coefficients is recovered by an iterative methodology with the guide of spatial connection in characteristic pictures so the head plaintext content is reproduced [10]. In another technique for versatile coding for encoded pictures, the first pixel esteems are veiled by a modulo-256 expansion to keep away from spillage of measurable data, prompting better security. The research work developed here is compressing encrypted images with an examination of AES and Chaotic Baker Map. In encryption stage, the data's are encoded by the proprietor. In compression stage, the data's in different DCT sub-groups are successfully packed by using quantization instrument without uncovering the original, and an advancement technique with proportion contortion criteria is utilized. At receiver end having the mystery key can reconstruct the original information. The results show that the execution of the twofold encryption techniques is enhanced.

The rest paper was prearranged in this way: Section 2 discusses proposed scheme of implementation and Section 3 explains performance metrics for evaluation. In Section 4, the output results are discussed continued with the conclusion in Sections 5.

II. PROPOSED SCHEME

In the proposed framework shown in Figure.1, a progression of pseudorandom numbers got from a secret key is utilized to encode the first pixel esteems [1]. After encryption, the picture is compacted utilizing DCT quantization technique. In the event that the substance is not exactly the necessary data transmission, at that point the pressure isn't required. While having the encoded bit streams and the mystery key, a decoder would first be able to acquire an estimated picture by unscrambling the quantized picture and afterward recreating the itemized substance utilizing the quantized coefficients with spatial association in general images. AES Encryption and Chaotic-Baker Map are utilized for the Encryption, which gives twofold encryption and gives more verified change.

Revised Manuscript Received on December 30, 2019.

* Correspondence Author

A.Mohanarathinam*, is currently working as Assistant Professor, Karpagam Academy of Higher Education, Coimbatore.
Email: mohanarathinam@gmail.com

S.Kamalraj, is currently working as Associate Professor, Karpagam Academy of Higher Education, Coimbatore. Email: kamalrajece@gmail.com

Prakash NB, is currently working as Associate Professor, National Engineering College, Kovilpatti. Email:nbprakas@gmail.com

Hemalakshmi GR, is currently working as Assistant Professor, National Engineering College, Kovilpatti. Email:grhemalakshmi@gmail.com

G.K.D.Prasanna Venkatesan, is currently working as Dean, Karpagam Academy of Higher Education, Coimbatore. Email: dean.engineering@kahedu.edu.in

A. Chaotic-Baker Map

Chaos can be defined as any state of disorder or randomness. However it has a much detailed meaning and significance when dealt scientifically [1]. Chaos can be characterized as any condition of disorder, confuse, or arbitrariness. It has a much detailed importance and hugeness when it managed deductively. On dynamical framework hypothesis, the baker‘s map was a disorderly guide from the unit square into it. The baker‘s map characterizes an administrator on the space of capacities. The baker‘s map was a precisely resolvable model of deterministic disorder, in that the Eigen capacities and Eigen estimations of the exchange administrator can be explicitly decided. It was an outstanding method of encryption to the picture preparing group. It was a transformation based instrument. Disordered Baker Map shows randomization of a square grid of measurements M×M by changing the pixel positions in view of a mystery key. In this technique, it relegates a pixel to another pixel position. It was an outstanding method of encryption to the image handling group. It was a permutation based device. Chaotic Baker Map displays randomization of a square grid of measurements by M×M, changing the pixel positions in terms of a secret key. In this strategy, it allocates a pixel to another pixel position. The discretized Baker outline indicated by B(v_1,v_2,… .,v_k), where B was the Baker guide and k was the arrangement of whole numbers, v_1,v_2,… .,v_k was chosen with the end goal that every whole number vi isolates by M, and Mi = v_1,v_2,… .,v_k.

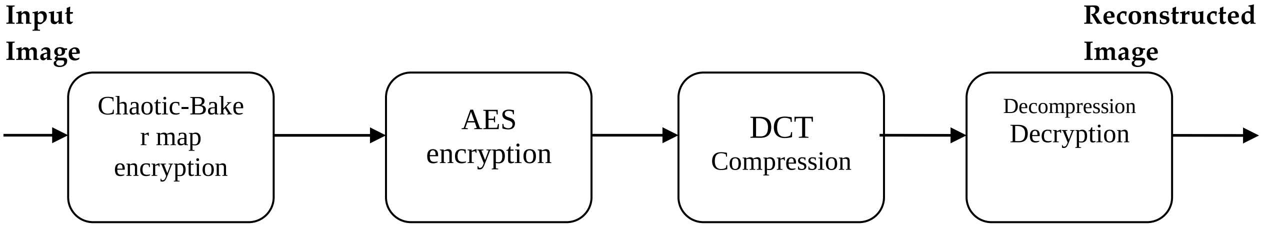

Fig. 1.Block Diagram for Double Encryption and Compression Method

B. AES Encryption

AES was a symmetric block cipher with a 128 bits piece size. AES depends on an outline rule known as a substitution-transform arrangement, blend of both programming and equipment. AES works on a 4×4 section significant network of bytes. The normal key volume of AES cipher requires a number of repetitions or iterations to convert the plaintext into cipher text. the AES encryption process was carried out by Rijndael architecture stated by Daemen and Rijmen (2013).

Here, each and every round encompasses different processing steps. To get back the original plaintext, a group of reverse rounds is used with the same encryption key. The AES performs different sub functions like sub bytes, mix columns, shift rows, add round key. The encryption of the data was carried out with add round key. The overall process was carried with diffusion and confusion. Diffusion refers to the designs in plaintext that were scattered in the cipher content. Confusion implies the connection between the plaintext and the cipher text was darkened.

C. Compression Techniques

When the channel capacity is sufficient, the encrypted image can be directly transmitted without any compression. At the receiver, original image can be retrieved from decryption of received image. When the channel capacity is limited, then image-compression is to be performed before transmission. The image compression was performed by 64 DCT sub-bands,

the coefficients of every sub-band were considered as a vector. Then orthogonal transformation was performed over the vectors.

Retrieval of original Image

The original image can be reconstructed at the receiver end by applying Inverse Discrete cosine transform. (IDCT). The retrieval process has the following stages.

- Apply Inverse DCT
- Apply AES decryption and Reversible Chaotic-Baker Map.
- Retrieved original image

III. PERFORMANCE METRICS

The investigation image of size 512×512 has used as the input image in this proposed work. The experimental results were evaluated by measuring performance of MSE, PSNR, compression-ratio, and correlation-coefficient.

PSNR

PSNR can be used to appraise an encryption scheme, which indicates the changes in pixel values between the actual image and the encrypted image.

$$PSNR= 10 \log 10(255^2/MSE) \qquad (1)$$

Correlation Coefficient

Correlation determines the relationship between two images. If correlation coefficient is same to 1, then two descriptions are equal and they may be in best association

Correlation coefficient (c.c) =corr2(x, y) (2)

Mean Square Error (MSE)

The MSE defined as the square of error between original image and retrieved frame. The distortion in reconstructed image is calculated by using MSE

$$MSE = \frac{\sum\sum[A(i,j) - B(i,j)]^2}{N \times N} \qquad (3)$$

Compression-Ratio

Compression reduces storage space and transmission bandwidth is measured by.

$$\text{Compression-ratio (C.R)} = \frac{\text{uncompressed image}}{\text{Compressed image}} \quad (4)$$

IV. EXPERIMENTAL RESULTS

The input image, the Chaotic-Bakered Image and the AES Encrypted Image samples are presented in Figure.2-Figure.4. Moreover, the compressed image, reconstructed image and the histogram analysis has been depicted in the Figure.5-Figure.7

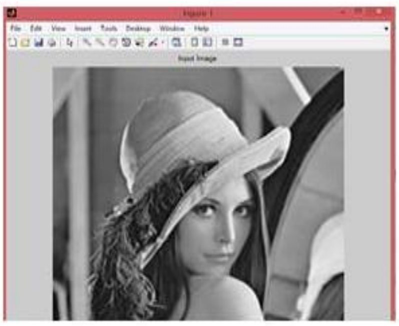

Fig.2 Input Image

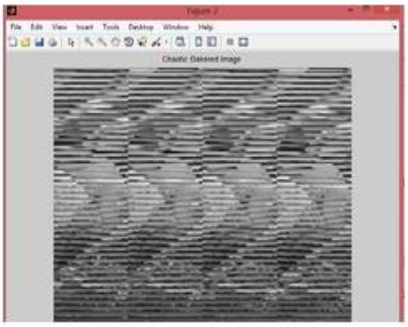

Fig.3 Chaotic Baker Map

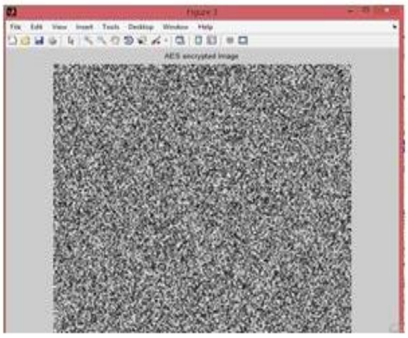

Fig.4 AES Encryption

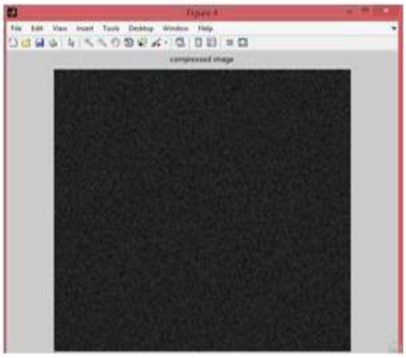

Fig 5 Compressed Image

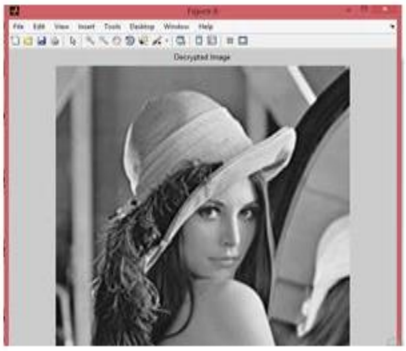

Fig 6. Reconstructed Image

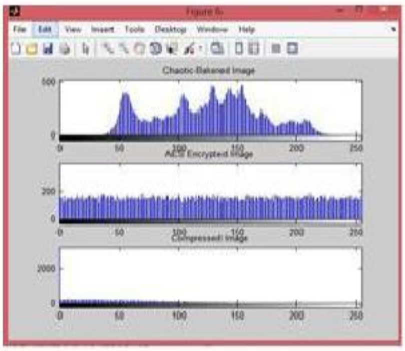

Fig 7.Histogram Analysis

The experimental results are tabulated in Table.1 shows an analysis of Compressing Encrypted Image with evaluated parameters. From the tabulation it was observed that double encryption technique produced better results than other techniques. The PSNR of Double encryption method is 57 % higher than the AES encryption and 78% higher than the Chaotic-Baker Map encryption.

Table.1 Comparison of encrypted images

Encryption Technique/image	C.R	PSNR	C.C	MSE
AES	0.5012	30.2138	-0.0019	61.901
Chaotic-Baker Map	0.5050	17.0654	0.0058	1.087e+03
Double encryption (Chaotic-Baker and AES Encrypted Image)	**0.83**	**77.1617**	**0.0011**	**0.0013**

V. CONCLUSION

In this research work, an image based double encryption scheme along with DCT compression technique has been proposed. The input image was encrypted by Chaotic Baker map and AES algorithms. The encrypted image was compressed by DCT compression technique. At receiver side, the image was reconstructed by performing decompression

and decryption using secret key. The proposed image based double encryption algorithm yields better results when compared with previous methods. The PSNR and MSE of proposed method was 77.1617 and 0.0013 respectively. The compression performance was also improved. This proposed scheme can be used for multimedia applications.

REFERENCES

1. R. Ramesh, J. Sunil Kumar, “Image Encryption and Compression Using Some Auxillary Information”, International Journal of Innovations in Engineering and Technology, Special Issue ETiCE 16-2016, pp.172-173.
2. Xinpeng Zhang, Yanli Ren, Liquan Shen, Zhenxing Qian, and Guorui Feng,”Compressing Encrypted Images with Auxiliary Information,” IEEE Transactions On Multimedia, 2014, vol. 16, no. 5. pp. 1327-1336.
3. X. Zhang, “Lossy compression and iterative reconstruction for encrypted image,” IEEE Trans. Inf. Forensics Security, 2011, vol. 6, no. 1, pp. 53–58.

4. W. Liu, W. Zeng, L. Dong, and Q. Yao, “Efficient compression of encrypted grayscale images,” IEEE Trans. Signal Process., 2010, vol. 19, no. 4, pp. 1097–1102..
5. D. Klinc, C. Hazayy, A. Jagmohan, H. Krawczyk, and T. Rabinz, “On compression of data encrypted with block ciphers,” in Proc. IEEE Data Compression Conference, 2009, pp. 213–222.
6. A. Kumar and A. Makur, “Distributed source coding based encryption and lossless compression of gray scale and color images,” Proc. IEEE 10th Workshop Multimedia Signal Processing, 2008, pp. 760–764.
7. A. Liveris, Z. Xiong, and C. Georghiades, “Compression of binary sources with side information at the decoder using LDPC codes,” IEEE Communications Letters, 2002, vol. 6, pp. 440–442.
8. N. Shulman and M. Feder, “Source broadcasting with an unknown amount of receiver side information,” in Proc. Inform. Theory Workshop, 2002, pp. 127–130.
9. M. Bellare, A. Desai, E. Jokipii, and P. Rogaway, “A concrete security treatment of symmetric encryption: Analysis of the DES modes of operation,” IEEE Proc. of 38th Annual Symp. on Foundations of Computer Science, 1997, pp.01-31.
10. D. Slepian and J. Wolf, “Noiseless coding of correlated information sources,” IEEE Trans. Info. Theory, 1973, vol. 19, pp. 471–480.

AUTHORS PROFILE

A.MOHANARATHINAM received B.E (Electronics and Communication Engineering) Degree from Bharathiar University, Coimbatore by the year 1999 and M.Tech (Electronics and Telecommunication Engineering) Degree from Janardan Rai Nagar Rajasthan Vidyapeeth University, Udaipur by the year 2008. She received her Ph.D Degree under the Faculty of Engineering (Research area: Image cryptography/steganography) from Karpagam Academy of Higher Education(Deemed to be University), Coimbatore by July 2019. She has more than 18 years of teaching experience and has published many papers in the reputed national and international journals and conferences. Her area of specialization includes image cryptography, image steganography, medical image processing and embedded systems.

KAMARAJ SUBRAMANIAM presently is working as Associate Professor in the Electronics and Communication Engg department at Karpagam Academy of Higher Education. He is also one of the executive members of the Human Machine Interface Cluster. He was involved in developing a prototype model of a Brain Controlled Wheelchair for Motor Neuron Disorder Patients. His Research Interest are Bio Signal Processing, Medical Image Analysis, Fractal Set Analysis, Very Large Scale Integration (VLSI), Mathematical Modeling and Algorithms, Artificial Neural Networks, Swarm Algorithms. He has been invited for guest lecturers in University Malaysia Perlis and Sri Ramakrishna Engg College.

N.B.PRAKASH received B.E Degree in Electrical and Electronics Engineering Department and M.E (Applied Electronics) Degree in Electronics and Communication Engineering Department from Madurai Kamaraj University, Madurai by the year 2000 and 2002. He received his Ph.D Degree under the Faculty of Information and Communication Engineering (Research area: Medical Image Processing) from Anna University, Chennai by June 2018. He has more than 17 years of teaching experience and has published many papers in the reputed national and international journals and conferences. His area of specialization includes medical image processing, pollution performance analysis in insulators and bushings, embedded systems and power system engineering. He is also an approved research supervisor under the faculty of Information and Communication Engineering of Anna University, Chennai bearing AU New Reference Number: 3340036 (S.No.763). He is also a peer reviewer in Elsevier, Springer, SCOPUS and SCI indexed international journals.

G.R.HEMALAKSHMI received her B.Sc (Computer Science) degree from Manonmaniam Sundaranar University, Tirunelveli by the year 2000. She received her Master of Computer Application Degree from Bharathiyar University, Coimbatore by the year 2003 and M.Tech (Information Technology) from Manonmaniam Sundaranar University, Tirunelveli by the year 2008. She is also pursuing research Ph.D program under the Faculty of Information and Communication Engineering (Research area: Medical Image Processing) at Anna University, Chennai since July 2017. She has more than 10 years of teaching experience and has published many papers in the reputed national and international journals and conferences. Her area of specialization includes medical image processing, Data Structures, and Programming languages etc.

G.K.D.PRASANNA VENKATESAN have got Combination of both Industrial Research and Development Experience from leading R and D Companies working mostly on Wireless networks on Physical layer. He has got Experience on Designing on 1XRTT CDMA Standards and 1XEVDO.Mostly interested to work on 3GPP Long term Evolution standard. Currently he is working as Dean, Faculty of Engineering, Karpagam Academy of Higher Education CEO I/c. His Specialties are Wireless Communication Networks, Design of RF Communication link and Adhoc networks. Sensor Networks, Embedded System.