A Novel Approach in Image Encryption Using AES Algorithm

Kaushal Kumar[1], Er. Jasdeep Singh Mann[2]
M.Tech Scholar[1], Assistant Professor[2]
Deptt. Of Computer Science, B.M.S.C.E., Sri Muktsar Sahib,Punjab (India)[1,2]
(kaushal_bit24@yahoo.co.in [1], erjasdeep.mann86@gmail.com [2])

Abstract : As the information trade in electronic way is quickly expanding, it is likewise similarly vital to shield the classification of information from unapproved get to. The breaks in security influence client's protection and notoriety. The information traded can be content, picture, sound, video and so on. Each sort of information has its own particular highlights and diverse methods are utilized to shield classified picture information from unapproved get to. Thus encryption of information is done to affirm security in open systems. Cryptography is the investigation of procedures for secure correspondence within the sight of a foe. It manages issues like encryption, validation, and key appropriation to give some examples. Image encryption is a system that gives security to pictures by changing over the first picture into a picture which is hard to get it. In the base paper, main approach was that they have added a key stream generator (A5/1W7) to AES to ensure improving the encryption performance; mainly for images characterized by reduced entropy. The implementation of both techniques has been realized for experimental purposes. Detailed results in terms of security analysis and implementation are given. Comparative study with traditional encryption algorithms is shown the superiority of the modified algorithm. But the comparative study showed that encryption time as well as decryption time of this algorithm is quite high. The parameters used in their research such as entropy, co-relation and PSNR are also needed to be analyzed. To improvise their algorithm, we have proposed an algorithm which deals with XOR operation of the sub keys. The methodology is described below.

Keywords: LEACH, PEGASIS, BFO, GA, DSR, PDORP, BS, ACO, WSN and nodes.

*****

I. INTRODUCTION

As the data exchange in electronic way is rapidly increasing, it is also equally important to protect the confidentiality of data from unauthorized access. The breaches in security affect user's privacy and reputation. The data exchanged can be text, image, audio, video etc. Each type of data has its own features different techniques are used to protect confidential image data from unauthorized access. Hence encryption of data is done to confirm security in open networks such as the internet where the multimedia applications are ever growing. Cryptography is the study of techniques for secure communication in the presence of an adversary. It deals with problems like encryption, authentication, and key distribution to name a few. Image encryption is a technique that provides security to images by converting the original image into an image which is difficult to understand. Applications of image encryption can extended to military communication, multimedia systems, medical science, telemedicine, internet communication etc. Generally images are different from textual data. The idea for encryption of image is to consider a 2D image as a 1D data stream and this stream is encrypted with any textual based crypto-system. This approach is called nave approach [1]. For text, small bit rate audio, image and video files that can be sent over a fast dedicated channel, this approach is suitable. Unfortunately these encryption algorithms may not satisfy for different image data types like JPEG, PNG, BMP, etc... i.e. Traditional crypto-systems can be used to encrypt images, but it is not a good idea as image size is always much greater than the textual data. Also the decrypted text should be equal to the original text, whereas this requirement is not necessary for image data. An image when decrypted contains small distortion and is usually acceptable because of the characteristic of human perception.

Imaging security and biometrics are two heavily connected areas in present day information security age. The quick evolution of biometrics with its usage in surveillance, verification and access control devices has raised the need of securing biometric data [1]. A majority of this image data from the biometric devices is visual, which has lead to intensive development of image security techniques for biometric applications [2]. Securing life forensic data over a communication channel and storing them must preserve the evidence by avoiding changes to the original image features such as the pixel values [3].

We chose Visual cryptography because it is the technique used to encrypt the data which is in the form of visual information such as images. Since the biometric templates stored in the database is usually in the form of images, the visual cryptography can be efficiently employed to encrypt the templates from attack [4].

II. RELATED WORKS

In 1989, Robert and Matthews proposed new encryption calculations decided from disorganized frameworks and owning to the basic properties of riotous frameworks, for example, the fragile dependence on starting conditions and pseudo-sporadic group which is hard to predict after a specific times of emphasis turbulent encryption [11].

Yang and Kim [18] proposed picture encryption and contrasting deciphering strategy relevant with security check. This strategy misuses a holographic procedure in that an encoded picture could be seen as a 3D picture illustration coming to fruition on account of impedance between two waves transmitted through a crucial ID picture and a reference picture serving as an encryption key. They have exhibited that their proposed technique conveys a honest to goodness regarded encoded picture, which empowers card manufacturing.

In 1996 [19], Scharinger and Pichler introduced another thing figure which scrambles enormous bits of plain substance by reiterated weaved use of substitution and change operations. The proposed arrangement used parameterizable changes on broad information pieces, (for instance, pictures) affected by specific cluttered structures.

In recent times, Yekkala et al. [86], used DCT change and versatile lightweight encryption strategy to encode chose hinders that contain edges. The idea behind their determination methodology is to scramble chose obstructs with pivotal data by using the point of confinement qualities at a specific extent, while the pieces having a place with different reaches are decoded. The PSNR regard of 14.46 db will be acquired, which interprets that a gatecrasher or assailant can't decode the mystery key used for the encryption.

In [88], the new strategy is presented utilizing three levels of change on chose squares and coefficients of orthogonal polynomials change area. The first picture will be initially disengaged into squares of 4 × 4 pixels and mixed them in three times. Firstly, scrambling chose bits through applying the orthogonal polynomials based change (OPT) then register the square of OPT coefficients. At that point the low level coefficients in OPT of every piece will be organized into a one dimensional crisscross arrangement. The pieces to be modified are chosen by pseudo-arbitrary grouping made utilizing a mystery sub-key as the seed. At last, the squares are part into subsets and revamped.

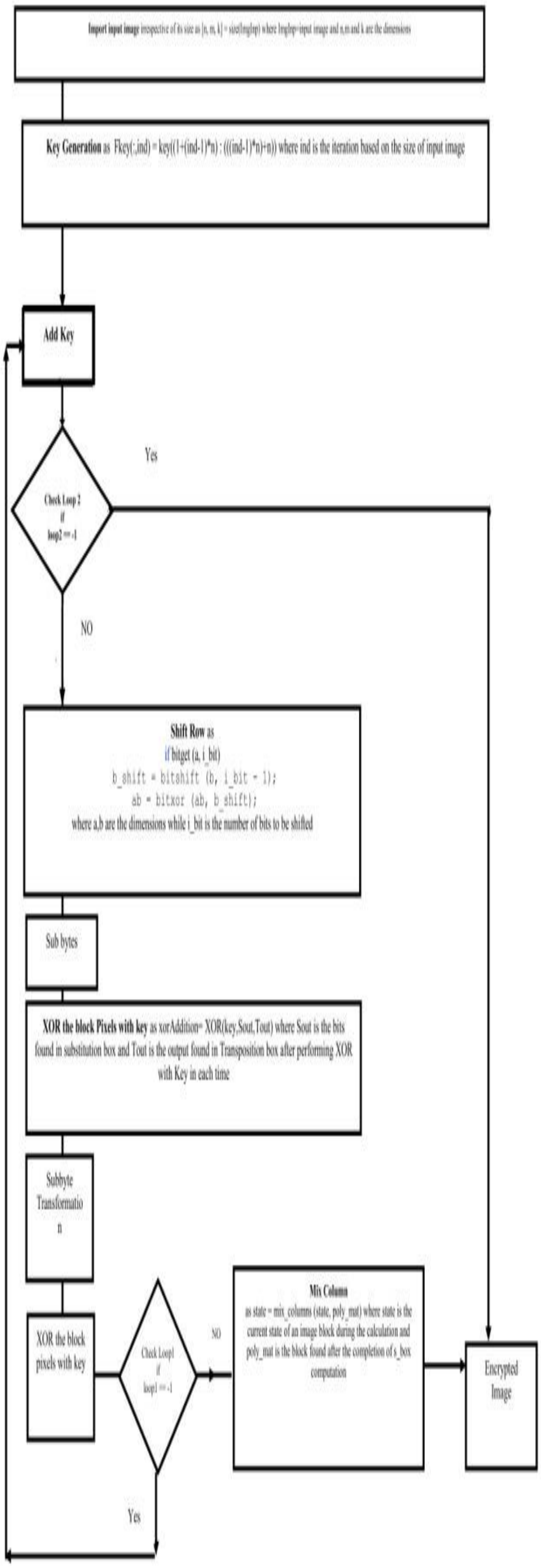
III. OBJECTIVE

Objective of of this research is as follows:

1. Working on AES (Advanced Encryption Standard) algorithm and implementing AES on image security.
2. Working on the limitations of precious works that including improving processing time, PSNR (peak signal to noise ration), entropy and correlation.

IV. FLOWCHART

Below is the flowchart of the proposed method:


Import input image irrespective of its size as [n, m, k] = size(ImgInp) where ImgInp=input image and n,m and k are the dimensions
Key Generation as Fkey(:,ind) = key((1+(ind-1)*n) : (((ind-1)*n)+n)) where ind is the iteration based on the size of input image
Add Key
Check Loop 2 if loop2 == -1
Yes
NO
Shift Row as
if bitget (a, i_bit)
b_shift = bitshift (b, i_bit - 1);
ab = bitxor (ab, b_shift);
where a,b are the dimensions while i_bit is the number of bits to be shifted
Sub bytes
XOR the block Pixels with key as xorAddition= XOR(key,Sout,Tout) where Sout is the bits found in substitution box and Tout is the output found in Transposition box after performing XOR with Key in each time
Subbyte Transformation
XOR the block pixels with key
Check Loop1 if loop1 == -1
NO
Yes
Mix Column as state = mix_columns (state, poly_mat) where state is the current state of an image block during the calculation and poly_mat is the block found after the completion of s_box computation
Encrypted Image

V. METHODOLOGY

Methodology for encryption process as follows:
Algorithm (with N = 2):
1.Read the input image and encode it using base64 standard.
2. Read the key file and initiate the AES 256 bit key using the hash (SHA-256) of key file.
3. Encrypt the image using the base 64 encoded text and hash generated in steps 1 and 2 respectively.
4. Create a new Image C of size (w, h) with pixel data p where
w - character support for key file (Default: 255)
h – Number of characters in the key file
p – Pixel Data to be filled (Default: 0)
5. For-each row i in height of image repeat:
a. Let j be ASCII code of the ith character in the key file.
b. Fill the first j pixels of the image in the ith row with black color .

6. Create N (= 2) Images (R, P) of the same size (w,h) and pixel data such that
a. For the first image R, pixel data is generated randomly. It can be either 0 (black) or 1 (white).
i. R[i][j]=random(0,1)
b. Second image pixel data P [i] [j] is defined such that
i. P [i] [j] = R [i] [j] xor C [i] [j] for every i, j in (h, w)
EncryptI

```
mage($Martrix_{red}$,$Matrix_{blue}$,$Matrix_{green}$,$M_R$,$M_G$,$M_B$,$FC_{red}$
,$FC_{grn}$,$FC_{ble}$,$FC_{key}$)

for i←i+1i ← 1, i ImageS ize/16 do
    $C_{red,i} \leftarrow Stream(i) \oplus FC \oplus M_R$
    $Cgreen,i \leftarrow Stream(i) \oplus FC \oplus MG$
    $C_{blue,i} \leftarrow S\ tream_{blue}(i) \oplus FC_{ble} \oplus M_B$
    if $i \bmod n(M_R) = 0$
    then
        $FC_{red} = AES(FC_{key}, FC_{ble})$
        $FC_{grn} = FC_{grn} \oplus FC_{red}$
        $FC_{ble} = FC_{ble} \oplus FC_{grn}$
    end for
    $i \leftarrow i+1$
end for

$CihperImage = CombineChannels(S\ tream_{red}, S\ tream_{green},$
$S\ tream_{blue})$
return CipherImage
endfunction
$CihperImage = CombineChannels(S\ tream_{red}, S\ tream_{green},$
$S\ tream_{blue})$
endfunction
```

where

Each data stream is masked using its corresponding key channel matrices generated in the previous section including M_R, M_G, M_B, FC_{red}, FC_{grn}, FC_{ble}, and FC_{key}.
Then, each color matrix is divided into 128-bit streams, each having 16 pixels of single color (red or green or blue as an image is consist of red, green and blue matrices) in its data. Following that, each of them is *Xor*ed with its correspondent first cipher (*FC*) and masker (*M*). When all data on the masker is used i.e. reached the end of maskers during this process, the *FC*s are updated using AES and bitwise *Xor*.
7. Output the encrypted encoding CI, Images P and R respectively.

Decryption

Algorithm (with N = 2):
1. Read the input cipher text of the image CI.
2. Load the Images K1, K2 from the input KI.
3. Create a new Image CK of size (w, h) same as K1, K2
such that
a. CK [i] [j] = K1 [i] [j] xor K2 [i] [j]
for every i, j in (h, w)
4. Initialize key K as an array of characters of size same as height of image CK (h).
5. For-each row i in height of image CK repeat:
a. Let count = 0
b. For each pixel j of the image in the i^{th} row with black color.
i. increment count by 1
c. Find the character ki by using ASCII code of the count generated after b. i.e., ki = char(count)
d. Set K[i] = ki
6. With the Key K initialize the AES 256 Algorithm with hash(K) (SHA-256)
7. Decrypt the cipher text CI and save the decrypted base64 encoding as an Image I
8. Output the decrypted image.

VI. RESULTS AND DISCUSSIONS

In the result and discussion section, we are implementing the proposed method in Matlab 2015b tool and discussing the results found along with performance analysis and graphical representation of the results found.
The image that are used in encryption process is as follows:

Fig: ina,Clown, Cheetah,Rose,Lisaw,Mouse

6.1 Results of different kind of images in Table form

Name of Image (Size)	**Encryption Time**	**PSNR**	**Entropy**	**Correlation (Horizontal)**	**Correlation (Vertical)**
Lena (256*256)	14.4685	5.9759	8.653	0.008635	0.0066352
Clown (200*320)	25.2355	3.0355	8.909	0.007018	0.0030178
Cheetah (200*320)	25.2959	6.0045	8.896	0.004693	0.0033931
Rose (256*256)	12.1804	2.5961	8.904	0.002748	0.0004479
Lisaw (256*256)	20.5738	2.4546	8.947	0.008903	0.0069032
Mouse (200*320)	12.434	4.3712	8.955	0.010068	0.0099323

6.2 Parameter results of Proposed Method in table form:

PSNR	**Correlation**	**Entropy**	**Throughput**
4.073	**0.0070108**	**8.8772**	**1560**

6.3 Encryption time comparison of results of proposed method with AES

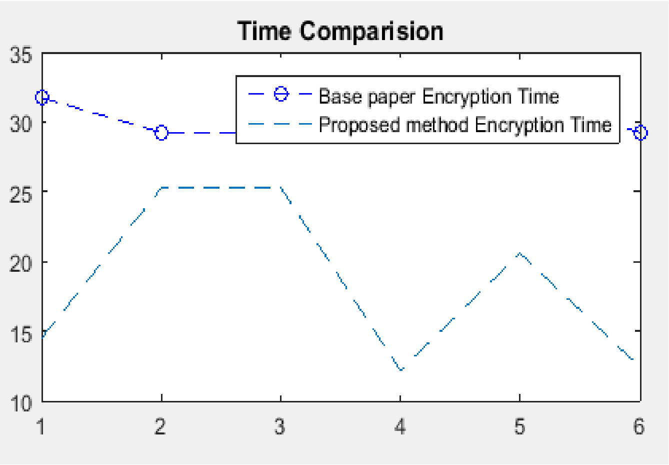


Fig 6 : Encryption time comparison of proposed method with AES

Method Name	Lena	Clown	Cheetah	Rose	Lisa	Mouse
AES	31.75	29.25	29.25	29.25	31.75	29.25
Proposed Method	14.468	25.235	25.296	12.18	20.574	12.434

Table : Encryption Time Comparison

6.4 Results Comparisons :

Parameter Name	**AES**	**AES+A5/1**	**AES+W7**	**Proposed Method**
Correlation	**0.046**	**0.056**	**0.02**	**0.0070108**
PSNR	**6.88**	**6.83**	**6.77**	**4.073**
Entropy	**7.91**	**7.96**	**8**	**8.8772**
Throughput	**1651**	**1646**	**1646**	**1560**

Table : Parameter Comparison

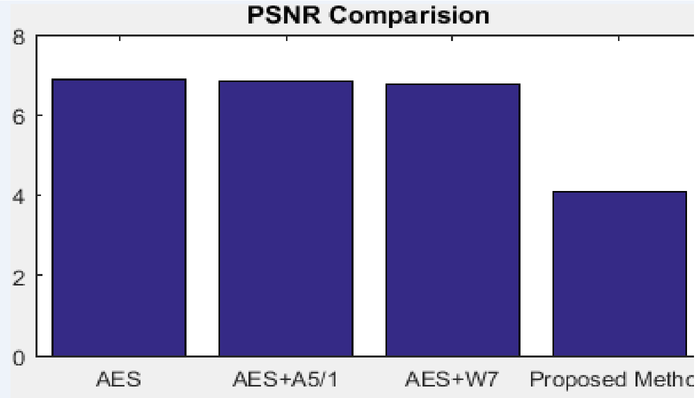


Fig : PSNR comparison

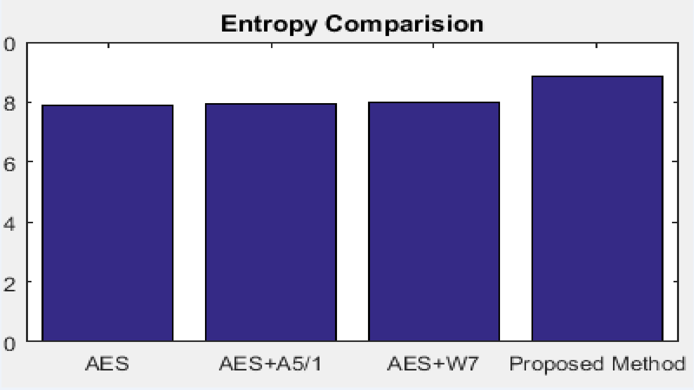


Fig : Entropy comparison

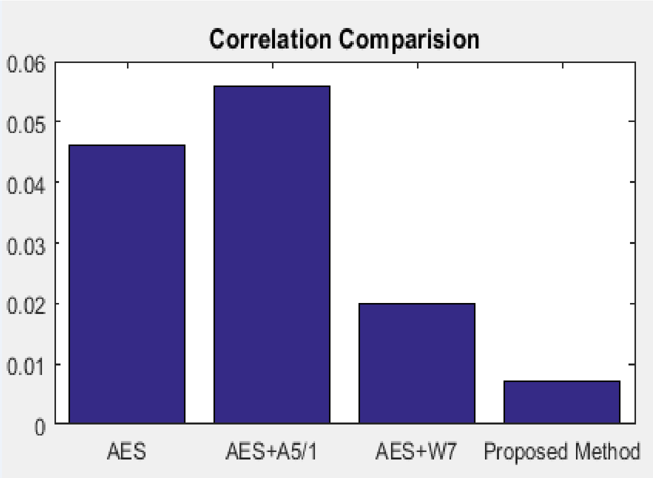


Fig : Correlation comparison

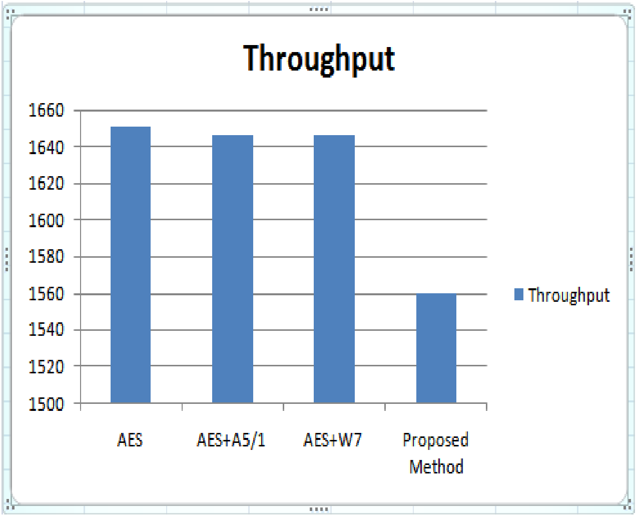


Fig : Throughput comparison

VII. CONCLUSION AND FUTURE WORK

This paper puts forward the method that use the AES algorithm with the key control to encrypt the image. This method incorporates a variety of characteristics, and with simple design. As the MATLAB has powerful numerical calculation function, especially for arrays and matrix calculations, and the infrastructure of the AES algorithm uses the matrix as the basic unit. So to implement the image encryption based on AES algorithm in the MATLAB environment is favorable. From the above experimental results and analysis, coupled key sensitivity analysis, this method can achieve very good effect on image encryption. And the decryption essence has the same structure with the encryption, so it can easily restore the original image. Due to the AES algorithm is easy to implement in software and hardware, it has laid a good foundation for subsequent image encryption in the transmission encryption on software and hardware. So we have reason to believe that use this method to encrypt the image will have a very good prospect in the future.

VIII. FUTURE WORK

Enhancing AES encryption method will be fruitful based on our method where key attention to be taken on reducing the iteration inside the algorithm.

IX. REFERENCES

[1] Alexopoulos, C., Bourbakis, N., & Ioannou, N. (1995). Image encryption method using a class of fractals. Journal of Electronic Imaging, 43, 251–259.

[2] Bao, G.-J., Ji S.-M., & Shen J.-B. (2002). Magic cube transformation and its application in digital image encryption. Computer Applications, 22(11), 23–25.

[3] Bourbakis, N., & Alexopoulos, C. (1992). Picture data encryption using scan patterns. Pattern Recognition, 25(6), 567–581.

[4] Chang, K.C., & Liu, J.L. (1994). An image encryption scheme based on quad-tree compression scheme. In Proceedings of the 1994 International Computer Symposium, Taiwan, (pp. 230–237).

[5] Communication theory of secrecy systems. The Bell System Technical Journal, 28, 656–715.

[6] Ding, W., Yan, W.-Q., & Qi, D.-X. (2000). A novel digital hiding technology based on Tangram Encryption. IEEE Proceedings of on NEWCAS 2005, and Conways Game. Proceeding of 2000 International Conference on Image Processing (Vol. 1, pp. 601–604), September 2000.

[7] Guibin Z, Changxiu C, Hu Zhongyu, et al. (2003). An image scrambling and encryption algorithm based on affine transformation. Journal of Computer-Aided Design & Computer Graphics, 15(6), 711–715.

[8] Habutsu, T., Nishio, Y., Sasase, I., & Mori, S. (1990). A secret key crypto-system using a chaotic map. Transactions of the IEICE, E73(7), 1041–1044.

[9] Jawad, L. M., & Sulong, G. B. (2013). A review of color image encryption techniques. International Journal of Computer Science Issues, 10(6), 266–275.

[10] Kuo, C. J. (1993). Novel image encryption technique and its application in progressive transmission. Journal of Electronic Imaging, 2(4), 345–351.

[11] Li, C.-G., Han, Z.-Z., & Zhang, H.-R. (2002). Image encryption techniques: A survey. Journal of Computer Research and Development, 39(10), 1317–1324.

[12] Menezes, A., van Oorschot, P., & Vanstone, S. (1996). Applied cryptography. Boca Raton: CRC.

[13] Rober, A., & Matthews, J. (1989). On the derivation of a “chaotic” encryption algorithm. Cryptologia, XIII(1), 29–42.

[14] Schwartz, C. (1991). A new graphical method for encryption of computer data. Cryptologia, 15(1), 43–46.

[15] Shannon, C. E. (1948). The mathematical theory of communication. The Bell System Technical Journal, 27, 379–423.Shannon, C. E. (1949).

[16] Sharma, M., & Kowar, M. K. (2010). Image encryption techniques using chaotic schemes: a review. International Journal of Engineering Science and Technology, 2, 2359–2363.

[17] Zhao, X.-F. (2003). Digital image scrambling based on the Baker’s transformation. Journal of Northwest Normal University (Natural Science), 39(2), 26–29.