ISSN: 0975-766X
CODEN: IJPTFI
Research Article

Available Online through
www.ijptonline.com

CIPHER AND DECIPHER OF IMAGE

E.Vijayan[1], N.C.Senthilkumar[2], J Nirmal Kumar[3], Mandakini Rastogi[4], I Himika[5]
School of Information Technology and Engineering (SITE), VIT University, Tamil Nadu, India.
Email: vijayvsi81@gmail.com

Received on 06-08-2016 *Accepted on 10-09-2016*

Abstract

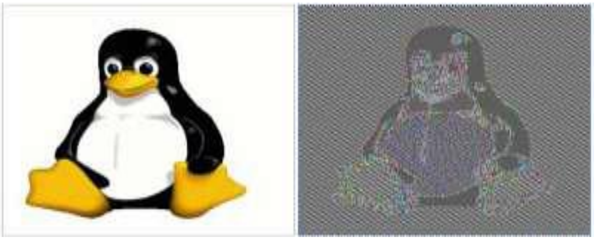
Today with the huge improvement of different advancements like mixed media, research on security is turning out to be more imperative. In giving security Cryptography puts an exceptionally pivotal part. Despite the fact that there are numerous cryptographic calculations to give security, they are not up to the attractive level of the clients. So there was a requirement for exploration on creating new calculations or changing existing calculations. In this paper we are going to explain about the traditional image cryptography technique commonly known as Visual Cryptography Scheme and then comparatively we have proposed an improved AES calculation for picture encryption which can be utilized to encode utilizing AES-128 bits key. The proposed changes in this paper are: repositioning the picture pixels to break the relationship between's them, randomization of key and concealing the key quality into the scrambled computerized picture and to apply a cover image. So the proposed system gives more security.

Keywords: Visual Cryptography, Advance Encryption standard (AES), Stamping.

1. Introduction

In this paper we are going to compare between the traditional image cryptography technique and the modern technique of image cipher. Visual cryptography is a dominant method which can offer higher security for any confidential information. This technique is generate noise like random pixels on share images to hide secret information which on overlay decrypt the information and commonly known as conventional visual secret sharing scheme. However, for avoiding such noise various methods has been used under Visual Cryptography Scheme most commonly the image synthesizer is used in an application where the receiver has to use the synthesizer to achieve the original secret images after the decryption. However, it is low potential and reliable with the existing systems of techniques like color images and animations etc.

With the quick improvement of multimedia innovation interactive media information like pictures, recordings, sounds are utilized as a part of different applications like entertainment, education, ads, and governmental issues. There are different types of encryption algorithms like AES, DES, and Blowfish etc. These algorithms are great at encoding content information yet coming to interactive media information these information are vast in volumes furthermore there is high excess.



Hence the security is low. This is on account of the connection between's the adjacent pixels in a picture can't be break by AES calculation. In real time application, we need better encryption calculation so we go for new encryption calculations or alteration to existing calculations. In this paper we presented another encryption calculation as a change to AES calculation. The modification is mainly focused to shifting pixel position, randomization of key for breaking the correlation between the image pixels and hiding the key into the encrypted digital image. For multimedia information the connection between's the picture pixels is too high, AES can't break this connection between pixels. In our improved AES algorithm we break the connection between the pixels by moving the pixel position line row and column wise. In our proposed algorithm we randomize the key values too.

2. Visual Cryptography Scheme

The Visual cryptography Scheme [1] used generating encrypted image here the original image is divided into 2 shares and each pixel of the image is converted into non-overlapping block of 2 or more sub-pixels in each of the shares. In Visual Cryptography Scheme (VCS)

[2] having one share will not be able to reveal any secret information so two or more shares are needed to higher the encryption and to reveal the secret information. There are many ways to encode the pixels of the secret image.

Visual cryptography is a powerful method which can provide higher security for any confidential information. This technique is generate noise like random pixels on share images to hide secret information which on overlay decrypt the information and commonly known as conventional visual secret sharing scheme.

This problem is solved using the EVCS (Extended Visual secret Cryptography Scheme that adds meaningful cover image in each share. But while removing extra cover images can be difficult as layers can intercept and violate to retrieval of the encrypted information or images.

EVCS in previous versions were used having the general access structures undergone with problem of pixel expansion. In spite of that a codebook design was needed for various schemes of the visual cryptography. Various approaches under the visual cryptography for the image encryption include:

1. Binary Images
2. Colour Images
3. Gray Images

2.1 Cryptography for Binary Images

Naor and Shamir's proposed a threshold (k,n) VCS where the given secret image is encoded into number of shadow images commonly called as 'shares' [5], here any key (i.e. 'k') or any more of them will be needed for decoder to decrypt the secret image , but many times (k-1) will not be able to recover the exact secret image as it may degrade the human visual system to illustrate the secret message by some overlapping share function and may produce noise in the resultant image and therefore overcoming the disadvantage of complex computation requires another robust technique for the image cryptography.

In image encrypting scheme the secret image data is entrenched into several images of shares of random binary pattern. Note that here the binary patterns of the shares have no visual definition and hinders the aim of visual cryptography. The researchers have imposed a better technique called 'half tone visual cryptography' that utilizes the void and cluster algorithm that encrypt the binary secret image into halftone shares (are images) having some visual information .Thus, this technique is better than the traditional visual cryptography scheme.

2.2 Visual cryptography for Colour Images

Another new cryptography introduced as for securing colour image based on visual cryptography scheme. Under this technique the colour image [7] has to be protected and the binary image is used as the key for encryption and decryption are taken as input data. Here the image is decomposed into monochromatic images that are converted into binary image data and then the binary images are encrypted using the binary key image known as share-l

That will provide binary cipher image. Finally to encrypt Exclusive OR operation is computed between binary key image and three half-tones of secret colour images separately. And for the decryption the shares are decrypted, also for the recovered binary images are inverse half toned and are combined to get binary secret image.

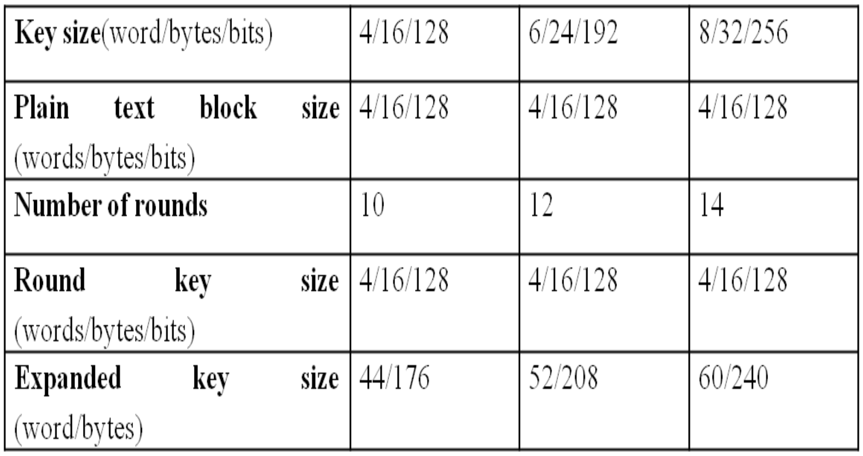
2.3 Visual Cryptography for Gray Images

In [6] the conventional encryption method the original secret digital image is divided into the n number of sub images and distributed into n o members in a group. In color cryptography scheme it includes the capabilities of watermarking an images and the verification. The method allows an N*N watermarking an image and embedding it into N*N secret image that construct two shadows and then verifies the accuracy of that reconstructed image. The verification is to determine the consistency of all the shadows before it is used for recovering the secret image avoids any member of the group from incidentally or intentionally provide the invalid data.

3. Advanced Encryption Standard

The Advanced Encryption Standard (AES) is a Symmetric square figure expected to swap DES for business applications. It utilizes a 128-bit block size and a key size of 128,192 or 256 bits, this standard which is a symmetric block cipher. The AES algorithm consists of four steps, which are executed one by one in a sequential manner by form rounds. The number of rounds will vary depend upon the key length.

3.1 AES Parameters



Key size(word/bytes/bits)	4/16/128	6/24/192	8/32/256
Plain text block size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Number of rounds	10	12	14
Round key size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Expanded key size (word/bytes)	44/176	52/208	60/240

The operations performed on fixed number of bytes in AES algorithm are classified as below

Add round key

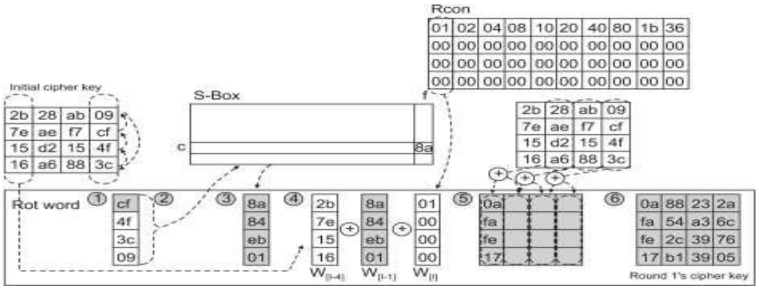
Bytes substitution

Shift rows

Mix column

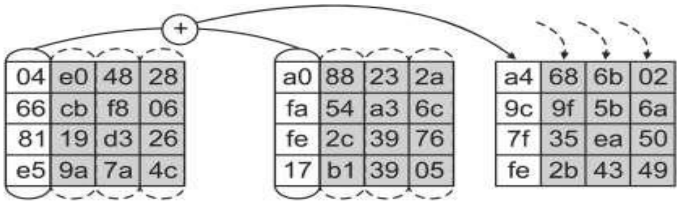
3.2 Key Expansion

The AES algorithm takes a key K, and performs a key Expansion routine by utilizing Rijndael'skey to create a key schedule. At the point when the key length is 128 bit, then the Key Expansion creates an aggregate 11 sub-key arrays of 128 bits, meant W_i and the first sub-key is the starting key. We require past sub-key, two tables, RCon and S-Box to create the sub-keys.



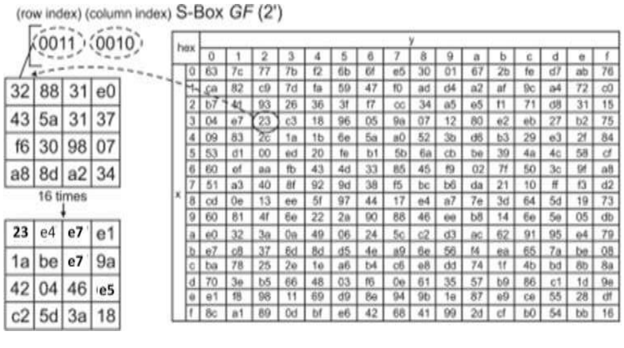
3.3 Add Round Key

In the AddRoundkey step, the sub-key is joined with the state. For every cycle, a sub-key is gotten from the fixed key by utilizing Rijndael's key schedule; size of the every sub-key is 128 bits. The sub-key is included by joining every byte of the state with the relating byte of the sub-key utilizing bitwise XOR as appeared as a part of below:



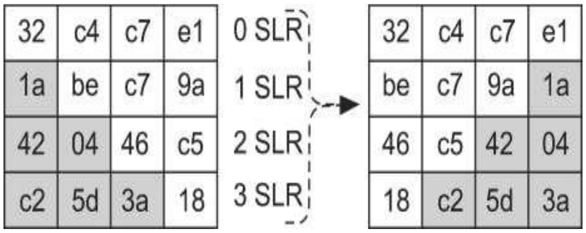
3.4 Sub Bytes

In the SubBytes step, every byte in the grid is supplanted with a SubByte using S-Box. This operation gives the non linearity in the cipher. The S-Box is drived from the multiplicative opposite over GF(2^8), known not great non-linearity properties. For instance the state network worth speaks to the line and segment lists of Sbox. Here in the underneath figure state grid esteem 32 speaks to the estimation of S-box at third line and second segment, so it substitutes 32 with 23



3.5 Shift Rows

The Shift Rows step works on the rows of the states; it consistently moves the bytes in every line by a certain offset. The primary row is left unaltered. Every byte in the three rows of the states is consistently moved more than 1, 2 and 3 bytes separately as demonstrated as follows



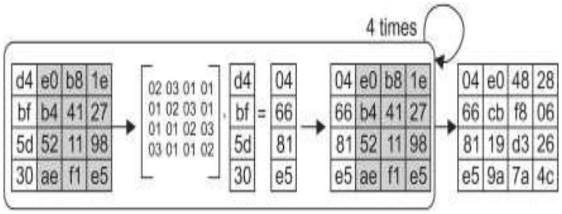
32	c4	c7	e1	0 SLR
1a	be	c7	9a	1 SLR
42	04	46	c5	2 SLR
c2	5d	3a	18	3 SLR

32	c4	c7	e1
be	c7	9a	1a
46	c5	42	04
18	c2	5d	3a

3.6 Mix Columns

In the MixColumns Step, the four bytes of every section of the state are joined utilizing an invertible direct change. It takes four bytes as data and yields four bytes, where every information byte influences each of the four yield bytes appeared in Fig. 5. During this operation, every column is multiplied by the known matrix that is:

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$



d4	e0	b8	1e
bf	b4	41	27
5d	52	11	98
30	ae	f1	e5

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \cdot \begin{bmatrix} d4 \\ bf \\ 5d \\ 30 \end{bmatrix} = \begin{bmatrix} 04 \\ 66 \\ 81 \\ e5 \end{bmatrix}$$

04	e0	b8	1e
66	b4	41	27
81	52	11	98
e5	ae	f1	e5

04	e0	48	28
66	cb	f8	06
81	19	d3	26
e5	9a	7a	4c

4. Literature Survey

Image stamping and synthesizing after sharing:

C Chandrasekar1 and K E Narayana used The Visual cryptography Scheme used generating encrypted image here the original image is shared ,then stamped then synthesized during decryption.

4.1 Superior quality Image Encryption Algorithm Based on AES Modification, 2014

SalimMuhsinWadi and NasharuddinZainal investigate the Advanced Encryption Standard and in their image encryption method they add two changes to AES calculation to enhance the execution and diminishing the equipment necessities. In the first place adjustment was led utilizing MixColumn change as a part of 5 rounds rather than 10 rounds, and the second alteration was as opposed to utilizing S-box and Inverse S-box as unique AES calculation they utilized stand out straightforward S-box for encryption and decryption

4.2 Adjusted Advanced Encryption Standard, 2014

PravinKawle, AvinashHiwase, GautamBagde, EkantTekam and Rahul Kalbande investigate the Advanced Encryption Standard (AES) and adjust it, to lessen the estimation of calculation and for enhancing the encryption execution. In adjusted AES calculation as opposed to utilizing Mixcolumn they utilize change on information. Changed AES calculation is a quick lightweight encryption calculation for security of media information. Every single above point of interest make calculation very suitable for the pictures and plaintext exchange also, than the AES algorithm.

4.3 Upgraded Image Encryption Techniques Using Modified Advanced Encryption Standard, 2012

Faisal Riaz, SumiraHameed, Imran Shafi, RakshanadaKausar and Anil Ahmed study the AES algorithm and give a change to the Existing AES calculation to build the speed of the AES calculation they proposed Selective Image Encryption procedure.

4.4 A new altered version of Advanced Encryption Standard based algorithm for image encryption, 2010

S.H.Kamali, R.ShakerianM.Hedayati and M.Rahmani investigate and introduce a change to the Advanced Encryption Standard to mirror an abnormal state security and better picture encryption. The alteration is finished by modifying the ShiftRow Transformation. Point by point results regarding security examination and execution are given. Trial results confirm and demonstrate that the proposed alteration to picture cryptosystem is profoundly secure from the cryptographic perspective. The outcomes additionally demonstrate that with a correlation to unique AES encryption calculation the adjusted calculation gives better encryption results regarding security against statistical attacks.

4.5 A Modified AES Based Algorithm for Image Encryption, 2007

M.Zeghid, M.Machhout, L.Khriji, A.Baganne, and R.Tourkimodify the Advanced Encryption Standard (AES), and include a key stream generator (A5/1, W7) to AES to guarantee enhancing the encryption execution; primarily for pictures characterized by reduced entropy.

5. Proposed Method

In our proposed calculation, we simply change the AES to be more productive and secure. For multimedia picture the connection qualities are too high which can't be evacuated by AES algorithm. So we have to break this nearby connection between these adjacent pixels. It can be accomplished by repositioning the pixel values. So we moved the pixel values row wise and column wise. This moving operation is done such a large number of times and we get our cipher picture which is not understandable. In our proposed method we by randomized the key values and moved the pixel values. Here we create key qualities relying upon the mouse position on the screen. At the point when the key length size is 128bits, there we require 16 values from the mouse position on the screen. So we take 8 mouse position values. In one position there is x position worth and y position esteem. We get this mouse positions and we get our sought key values. At that point we have done our encryption by utilizing these key valuesas a part of our proposed technique we randomized the key worth which is crucial piece of the decryption. In the event that we don't have the idea about the key valuethen we can't decode the picture. So we have to send this key value with encrypted picture. So with this key value and cipher picture we create another picture this picture is to be stamped with another using Block Based Transformation Algorithm to add security to the image. This stamped picture is our desired encrypted picture.

6. Detailed Alogorithm :

6.1 Ciphering Algorithm

Steps:

1. The picture document is taken as the info.
2. The pixels are correct moved along row wise and column wise to break the relationship between's the adjacent pixels and accordingly the first level figure picture can be acquired.
3. Key value is produced arbitrarily.
4. A key Expansion routine is to be performed by utilizing Rijndael's key timetable to produce a key schedule. At the point when the key length is 128 bits, then the Key Expansion produces an aggregate 11 sub-key varieties of 128 bits, indicated Wi and the first sub-key is the beginning key.
5. The sub-key is joined with the state. This step is known as AddRoundkey Step. For every cycle, a sub-key is gotten from the fixed key by utilizing Rijndael's key schedule. Size of the every sub-key is of 128 bits.
6. Each byte in the matrix is replaced with a SubByte utilizing S-Box. This operation gives the non linearity in the cipher. The S-Box is gotten from the multiplicative opposite over GF(28) to have great non-linearity properties.
7. The bytes in every row are consistently left moved by a offset where the first row is left unaltered.
8. The four bytes of every column of the state are consolidated using an invertible linear transform. It takes four bytes as data and yields four bytes, where every byte influences each of the four output bytes.

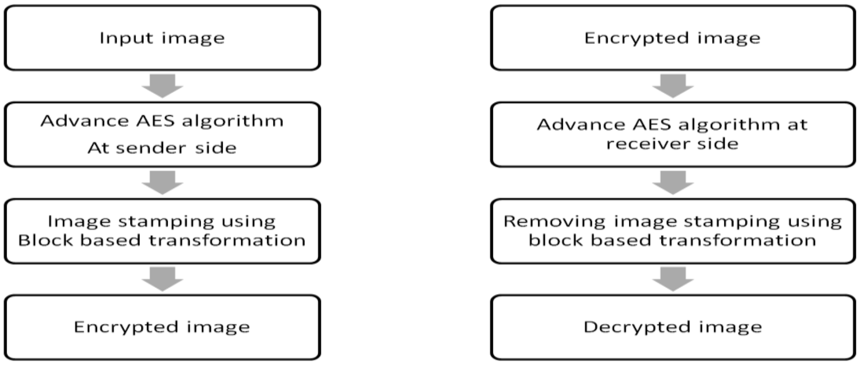
9. The AddRoundkey Step operation is repeated again.
10. Step 6 -9 operations are to be repeated for eight times and in the last round step 6, stage 7 and step 9 operations will be repeated.
11. The second level encrypted picture is then produced by utilizing the key qualities and the first level figure picture, which can be exchanged through open reason correspondence channel.
12. Output from modified AES is added a cover image called stamping [9] using Block Based Transformation Algorithm. Stamped image can be taken as input from the user.

6.2 Deciphering Algorithm

Steps:

1. Here user gets the stamped encrypted image, so the stamp should be removed to decipher the image.
2. Upon getting the stamp removed cipher picture the decoding or extraction procedure can be began.At first, from the second level cipher picture the key value to be removed.
3. A key Expansion routine is to be performed by utilizing Rijndael's key schedule to create a key schedule. At the point when the key length is 128 bits, then the Key Expansion creates an aggregate 11 sub-key varieties of 128 bits, denoted Wi and the first sub-key is the intial key.
4. The sub-key is consolidated with the state. This step is known as Inverse AddRouudkey Step. For eachround, a sub-key is drived from the fixed key by utilizing Rijndael's key schedule. Size of the every sub-key is of 128 bits.
5. The bytes in every row are consistently right moved by a certain offset where the first column is left unaltered.
6. Each byte in the matrix is replaced with a SubByte using S-Box. This operation gives the non linearity in the figure. The S-Box is gotten from the multiplicative opposite over GF (28) to have great non-linearity properties.
7. The Inverse AddRouudkey Step operation is repeated again.
8. The four bytes of every segment of the state are joined utilizing an invertible direct change. It takes four bytes as information and yields four bytes, where every byte influences each of the four output bytes.
9. Step 4- 7 operations are to be repeated for eight times and in the last round, step 4, stage 5 and step 6 operations will be repeated.
10. The pixel values are left moved along row and column wise for repositioning the pixel values.

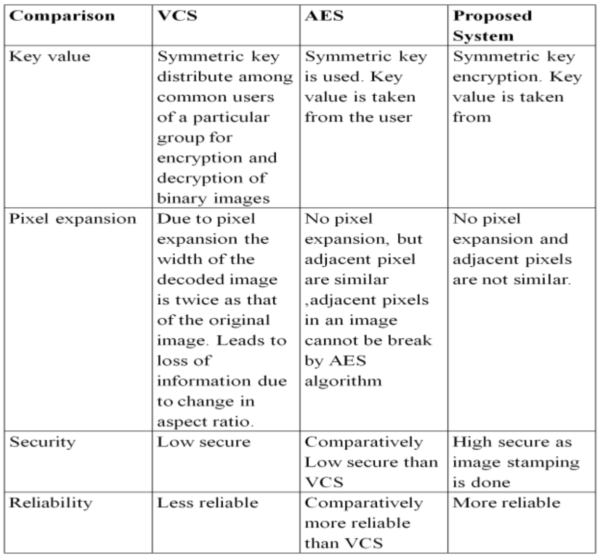
11. Finally the first picture can be acquired.


Input image
Advance AES algorithm At sender side
Image stamping using Block based transformation
Encrypted image
Encrypted image
Advance AES algorithm at receiver side
Removing image stamping using block based transformation
Decrypted image

A) Ciphering Step **B) Deciphering Step**

Figure:Steps involved in cipher and Decipher of image.

7. Comparison Between Visual Cryptography, Advance Encryption Standard And Proposed System.



Comparison	VCS	AES	Proposed System
Key value	Symmetric key distribute among common users of a particular group for encryption and decryption of binary images	Symmetric key is used. Key value is taken from the user	Symmetric key encryption. Key value is taken from
Pixel expansion	Due to pixel expansion the width of the decoded image is twice as that of the original image. Leads to loss of information due to change in aspect ratio.	No pixel expansion, but adjacent pixel are similar ,adjacent pixels in an image cannot be break by AES algorithm	No pixel expansion and adjacent pixels are not similar.
Security	Low secure	Comparatively Low secure than VCS	High secure as image stamping is done
Reliability	Less reliable	Comparatively more reliable than VCS	More reliable

8. Results

Other than giving high confirmation capacity and great power, this proposed plan gives great recoverability. On the off chance that we utilize our proposed strategy we get the outcomes as demonstrated as follows .Here the cipher pictures are absolutely invisible and use of Block based transformation for stamping of image.

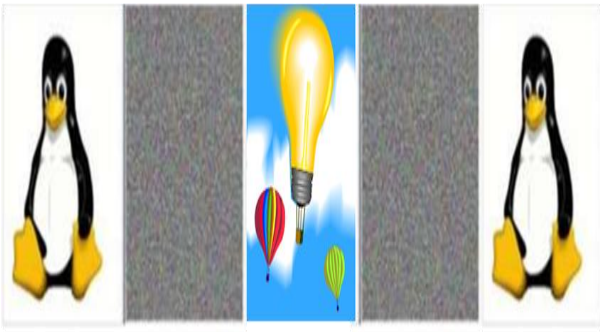


Figure: a)input image b)AES ciphered image c)Stamping d)image after removing stamp e) deciphered image.

9. Conclusion

In this paper we modified the AES algorithm and we proposed a new algorithm. The adjustment is finished by randomizing the key values and repositioning the pixel values. We have demonstrated that the proposed cryptosystem gives better encryption results as far as security against measurable attacks. If it gives great security statistical analysis it takes more time. So we suggestreducing the number of rounds in AES algorithm for decrease the time complexity and then stamping of image to make the encryption high secure.

References

1. "Visual cryptography, M. Naor and A. Shamir-1994.
2. "New visual secret sharing schemes using probabilistic method", C. N. Yang-2004
3. "Step construction of visual cryptography schemes", F. Liu, C. Wu, and X. Lin-2010.
4. "A Survey on Visual Cryptography Techniques and their Applications", Ms BhawnaShrivas and Prof.Shweta Yadav.
5. Zhi-hui Wang, Chin-Chen Chang, Huynh Ngoc Tu, "Sharing aSecret Image in Binary Images with Verification" Journal ofInformation Hiding and Multimedia Signal Processing Volume 2,Number 1, January 2011.
6. "Visual Cryptography Schemes for Secret Image Sharing using GAS Algorithm",Bharanivendhan N and Amitha T.
7. "Visual Cryptography Schemes for Secret Color Image Sharing using General Access Structure and Stamping Algorithm"
8. "Various Problems in Visual Cryptograph."
9. "Two Step Share Synthesized Image Stamper Agorithm for Secure Visual Sharing ",CChandrasekar and K E Narayana.

Corresponding author:
E.Vijayan*,
Email: *vijayvsi81@gmail.com*