Volume 5, Issue 8, August 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Symmetric Diffusion-Double Substitution Based Image Encryption

S. Vani Kumari
Asst. Prof in CSE Department
GMRIT, Rajam, India

Abstract-Security of images has become very important for many applications like video conferencing, secure facsimile, medical, military applications etc. It is hard to prevent unauthorized user from eavesdropping in any communication system including internet. To protect information from unauthorized user, mainly two different technologies are used. These are - digital watermarking and cryptography. These two technologies could be used complementary to each other.

A new image encryption scheme using a secret key of 128-bit size is proposed. In the algorithm, image is partitioned into several key based dynamic blocks and further, each block passes through the eight rounds of diffusion as well as substitution process. In diffusion process, sequences of block pixels are rearranged within the block by a zigzag approach whereas block pixels are replaced with another by using difference calculation of row and column in substitution process. The above mentioned process have 16 rounds. Due to high order of substitution and diffusion, common attacks like linear and differential cryptanalysis are infeasible. The experimental results show that the proposed technique is efficient and has high security features.

Keywords- encryption;substitution;diffusion;cryptanalysis;

I. INTRODUCTION

Fast growing internet which is powered by even faster computing systems demands higher speed and security. Providing real time security is difficult because encryption and decryption take lot of time. In order to provide real time security innovative techniques are required. The security of digital images has attracted more attention recently and different encryption methods have been proposed to enhance security of images[2].

Encryption is a common technique used to secure images. Image and video encryption has many applications in internet communications, multimedia systems, medical imaging, satellite imaging and military communications. Image encryption techniques try to convert an image to another one that is hard to understand. On the other hand, image decryption retrieves the original image from the encrypted one.

Many encryption algorithms are already developed which provide strong security to images. But they fail to work in real time scenario. Image encryption is different from text encryption because of its own characteristics. Hence we develop a project "Symmetric diffusion-double substitution based image encryption" which provides an efficient algorithm for encrypting images which takes low computation power. The main concern of this project is to provide security to images at higher level. We degrade image quality before applying encryption process. During encryption image is divided into blocks on which diffusion and substitution are performed. Instead of single confusion method, we are applying confusion for two times to make encryption stronger.

II. BACKGROUND STUDY

Narendra K. Pareek et al proposed an encryption algorithm for gray images. The proposed algorithm uses a 128 bit-key. Initially, visual quality of the image is degraded by the Mixing process. Resultant image is divided into non-overlapping squared dynamic blocks. These blocks are passed through key dependent Diffusion and Pixel Substitution processes[6]. The Diffusion and Pixel Substitution processes are performed successively for sixteen rounds. Further, all the blocks are merged to form a single image which is passed through Row-Column Substitution process 36[6]. The proposed encryption scheme is easy to implement and provides high encryption rate. Different experimental results and analysis have been done to approve the high security features and effectiveness of the proposed encryption scheme.

A data transmission system is said to reliable if provides security to the data being transmitted against any type of security attacks such as modification, fabrication, replay etc. With the advancement in computer networks and information technology, a huge amount of digital data is being exchanged over various types of networks. Major part of transmitted digital data, which is either confidential or private, demands for security mechanisms to provide required protection [3]. Therefore, security has become an important issue during the storing and transmission of digital data. In secured communications using cryptography, the information under consideration is converted from the intelligible form to an unintelligible form at sender end. Encryption process scrambles the content of data such as text, image, audio, and video to make the data unreadable or incomprehensible during transmission. The encrypted form of the information is then transmitted through the insecure channel to the desired recipient. At the recipient end, the information is again converted back to an understandable form using decryption process.

Digital gray images are various medical applications like magnetic resonance images (MRIs), computed tomography (CT), X-rays images, etc and even used in military operations also. Medical applications often deal with patients' data that are confidential and should only be accessible to authorized persons. While some patients are unconcerned about breach of confidentiality could cause extreme embarrassment, humiliation and even loss of employment. Therefore, there is a need to protect and maintain confidentiality of patient's records stored as well as those of any kind of transmission of such data.

Several well-known text encryption algorithms such as substitution techniques, transposition techniques, RSA, DES, Triple DES, IDEA Etc. algorithms can be used to perform the image encryption and decryption. But, they appear not to be ideal for image applications, due to some intrinsic features of images such as bulk data capacity, pixel correlation and high redundancy. They take much computational time. In this situation, we propose a new technique that gives an efficient and ideal image encryption algorithm. Using this technique, we first divide the image into blocks, shuffle the blocks and pixels to decrease correlation and then encrypt an image using chaotic logistic maps.

Very few image encryption algorithms, exclusive designed for digital gray images, are seen in literature. When same key is used in encryption and decryption process, such algorithms are grouped under symmetric key cryptography. Numerous symmetric image encryption schemes based on different approaches are available in literature. There is a need for the development of mechanisms which provides high security and encryption rate in the applications related to the fields of military and medical sciences. Our proposed encryption scheme mainly focuses on the security level and encryption rate of the data that to be transmitted.

Particularities of Image encryption: Unlike text messages, image data have special features such as bulk capacity, high redundancy and high correlation among pixels, not to maintain that they usually are huge in size, which together make traditional encryption method difficult to apply and slow to process. Sometimes image applications also have their own requirements like real time processing, fidelity reservation, image format consistence, and data compression for transmission. Simultaneous fulfilments of these requirements, along with high security and high quality demands, have presented great challenges to imaging practice. One example is the case where one is to manage both encryption and compression. In doing so if an image is to be encrypted after its format is converted, say from a TIFF to GIF file, encryption has to be implemented before compression. However, a conventional encrypted image has a very little compressibility. On other hand, compression will make a correct and lossless decipher impossible, particularly when the highly secure image encryption scheme is used. This conflict between the compressibility and security is very difficult, if not impossible, to complete resolve.

In terms of security, image data are **not as sensitive** as text information. Security of images information is relatively low, except in some specific situations like military and espionage applications or video conference in business. A very expensive attack of encrypted median data is generally not worthwhile. In practice, many image applications do not have very strict security requirements. Under certain circumstances, protection of the fidelity of an image object is more important than secrecy. An example is electronic signature. As another example, in image database applications, only those users who have paid for the service can access to large size images with high resolution. Adversaries may be able to get some small size images with low resolution by attacks based on cryptanalysis, but those images have little business value and perhaps much cheaper than the cost of preparing and executing the attacks

Today, there does not seem to be any image encryption algorithm that can fulfil all the aforementioned specifications and requirements.

Diffusion and substitution image encryption, cannot solve all these problems either. However, it can provide a class of very promising methods that can partially fulfil many of these requirements and demonstrate superiority over the conventional encryption methods, particularly with a good combination of speed, security, and flexibility. As seen below, through an elaborative design, either block cipher or stream cipher can achieve very good overall

III. PROPOSED ALGORITHM

In our proposed algorithm image is degraded before applying encryption using XOR operation with previous pixels. Generate a 128 bit hexadecimal key. Each four bit are called subkey and each 8 bit are called session keys.

Then the following steps are applied for each iteration.

Divide the image into equal number of blocks where the number of blocks are decided by the session key. Now take each block and apply diffusion method(Scramble the pixel in a zigzag manner).Now apply substitution method this method each pixel value is modified with one of its 8 surrounding pixels. After applying the 16 iterations combine the blocks into single image [1]. Now apply Row-Column substitution on the entire image. The resulting image is the encrypted image. Fig-1 represents the flow of the entire process involved in the encryption.

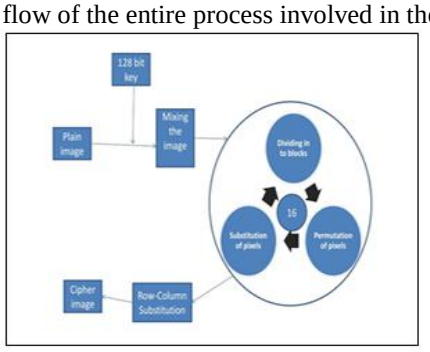


Figure:1

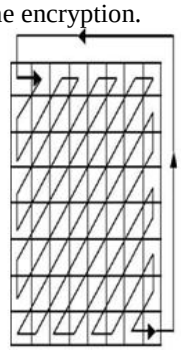


Figure.2

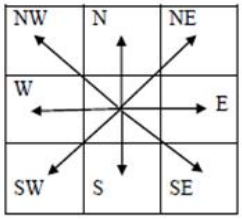


Figure.3

Pixel Mixing:

In mixing process, each pixel is replaced with the pixel obtained by performing XOR operation between the current pixel, the previous pixel and session key [1]. For first pixel, since there will be no previous pixel so in place of previous pixel we use zero.

for x=1:H do
  for y=1:W do
    $P_{X,Y}=(P_{X,Y}$ XOR $P_{X,Y-1})$ XOR k_i
i=(i mod 16)+1
end for
end for

Zig-zag scrambling

1.Take each divided block as input.
2.Traverse the image as shown in Figure.2
3.Change the position of pixel in the traversing order.

Substitution with surrounding pixel

In this process, properties of the pixels of each block are altered with one of their surrounding pixels. The chosen adjacent pixel to the current pixel is one of the pixels located at the eight possible adjacent locations i.e. East(E),North–East (NE), North (N),. . . as shown in Fig. 3. To change the properties of current Pixel (Pi, j), we choose one of its adjacent pixels ($P_{x,y}$) and XOR it with current pixel ($P_{i,j}$).

The selection of pixel ($P_{x,y}$) depends on the key used in the algorithm as shown in Table 4.3. Properties of the pixels of a block are altered sequentially row by row. We use subkeys k_1,k_2,k_3, . . . to alter the properties of first, second, third, . . . ,pixels respectively. When all the sub-keys are exhausted, start the process from the first sub-key k_1 again. In this step, some of the pixels lying on the boundary of a block may be remain unaffected.

Row-column substitution:

1.Take the image as input.
2.For each row identify the maximum value and modify each pixel value by subtraction of the pixel value from the maximum value.
3.Next, for each column identify the maximum value and modify each pixel value by subtracting the pixel value from the maximum value.

Encryption

(1)The algorithm uses a 128-bit key. The key can be generated randomly. The key can be divided into blocks of size 8-bits(Hexadecimal digits), each such block (ki) is referred to as sub key i.e., the key contains 32 sub keys.
here ki's denotes sub keys and Ki 's represents session keys.
(2)First, plain image passes through the mixing process)which degrades the quality of original image or distorts it.
(3)For L=1:16

Divide the obtained image from the mixing process into non-overlapping squared blocks, i.e.,B1,B2,B3,.. BN. The size of each block used in the round depends on the Session Key(KL) used in the round. The total number of blocks(N) obtained will depend on the size of the image to be encrypted.

a)For p = 1 : N do
  i.Block (B p) passes through the diffusion process with sub-key pair (kx, ky).
  ii.Resultant block passes through the pixel substitution process. end For

(4)The blocks are combined to form a single image. The resultant image will pass through Row-Column substitution process.

Inverse Row-Column Substitution

1.Take the image as input.
2.For each column identify the maximum value and modify each pixel value by adding the pixel value with the maximum value.
3.Next, for each row identify the maximum value and modify each pixel value by adding the pixel value with the maximum value.

Inverse Pixel Substitution

1.Take the image as input.
2.In this the properties of the pixel are modified by performing XOR with one of the adjacent pixels. The adjacent pixel can be chosen based on table.
3.In this the traversing is done in the order opposite to the order traversed in the process Pixel Substitution (0).

Inverse Zig-Zag Scrambling

1.Take the image as input.

2.Traverse in the reverse order of the pixels traversed in the Zig-Zag Scrambling process. Inverse Pixel Mixing

In Inverse Pixel Mixing process, each pixel is replaced with the pixel obtained by performing XOR operation between the current pixel and the Session Key and the obtained result is XORed with the previous pixel value. For first pixel, since there will be no previous pixel so in place of previous pixel we use zero.

```
for x=1:H do
   for y=1:W do
         PX,Y=( PX,Y xor ki) xor PX,Y-1
         i=(i mod 16)+1
   end for
end for
```

Decryption

(1)The encrypted image is passed through inverse Row-Column Substitution.

(2)For L=16:1

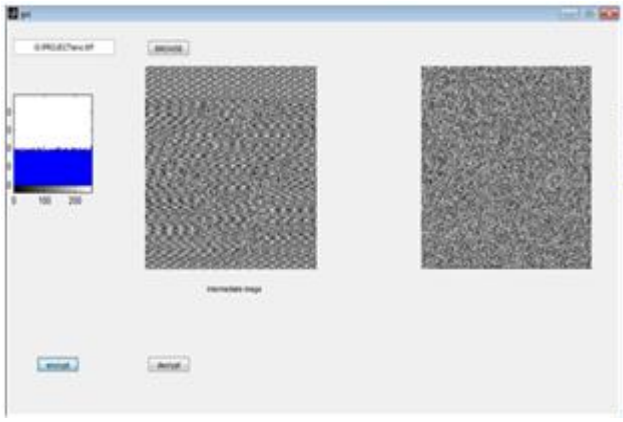
Divide the obtained image from the mixing process into non-overlapping squared blocks, i.e.,B1,B2,B3,.. BN based on the session key(KL).

(i)Each block(Bp) passes through inverse pixel substitution method.

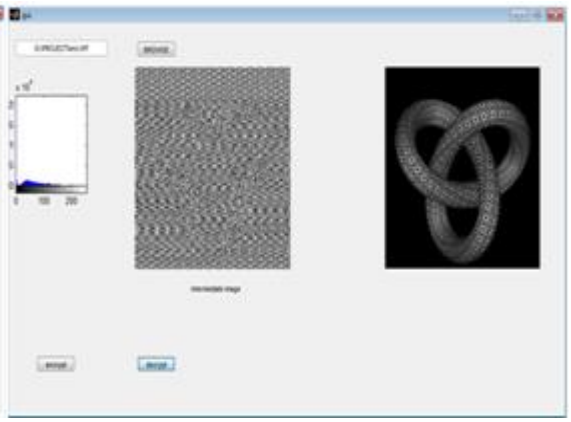
(ii)Then each block is passed through inverse diffusion process.

(3)The blocks are combined to form a single image. The resultant image is passed through inverse Mixing process. The original image used for encryption will be obtained.

IV. EXPERIMENTAL RESULTS



Displaying encrypted image and it's histogram



Original image after decryption and its histogram

Performance analysis:

For an image encryption algorithm, its performance mainly depends on the entropy, correlation and the time taken for encryption

Entropy: Entropy is a statistical measure of randomness that can be used to characterize the texture of the input image. Entropy is defined as Where p is the vector containing the frequency of each intensity level in the image. Entropy for the current algorithm for various images comes nearly as 7.99 which is almost the ideal case .

Correlation: Correlation determines the relationship between the two entities. If two entities increases either monotonically or decreases monotonically they are respectively said to have positive or negative correlation. Our encryption algorithm gives correlation that is almost null meaning that original and encrypted image are not related to each other.

Time taken for encryption: General encryption methods like DES,AES and RSA takes more time to encrypt an image i.e. 3-5 minutes since they are not ideal for image encryption. But our encryption scheme takes less than 7 seconds to encrypt an image of size 300x300. Table 7.1 shows the comparison of time taken encrypting image by various algorithms

Table comparing time taken for encrypting image by various algorithms.

Image size	**Proposed Algorithm**	**AES**	**RSA**
150X150	1.83 sec.	42 sec.	100 sec.
300X300	7.4 sec.	40 sec.	260 sec.
500X500	20.5 sec.	220 sec.	400 sec.
1024X1024	89 sec.	160 sec.	860 sec.

IV. CONCLUSION

As present world is more concerned about the security so we proposed a high level secure image encryption scheme- Symmetric Diffusion and Double Substitution. The proposed encryption scheme takes gray image as input and generates a high level secured image. First the quality of the image is degraded by applying the Pixel Mixing process. Then the partial encrypted image is divided into several non overlapping squared key dependent blocks. After that each block pass through diffusion and pixel substitution. In diffusion the pixels of the image are scrambled using zig-zag path which enhances the security of the encrypted image. In Pixel Substitution each pixel properties are altered by performing XOR with one of the adjacent surrounding pixel. In Row-Column Substitution block pixels are replaced with another by using difference computation of rows and column pixels. The size of the key can easily increased. It provides loss less encryption of images, symmetric private key encryption with sufficient key space. Encryption and Decryption uses Exclusive-OR which can be easily implemented in hardware. We performed Histogram analysis, Entropy analysis, pixel correlation analysis. Based on the results of our analysis, we conclude that the proposed image encryption technique is perfectly suitable for the secure image storing and transmission

V. FUTURE WORK

Extension to RGB image: We have developed the encryption scheme to gray image. It can also be applied to RGB images by extracting each color component and applying the encryption algorithm to them.

Compression: Since we are applying the encryption on gray scale image, it is possible that pixels in a particular area can be of the same intensity levels. So we can divide the image into blocks and can apply compression techniques on the blocks.

REFERENCES

[1] Narendra K. Pareek, Vinod Patidar, Krishan K. Sud, Diffusion–substitution based gray image encryption scheme, Elsevier Inc. (2013) .

[2] Ali B.Y. Mohammad, J. Aman, Image encryption using block based transformation algorithm, IAENG Int. J. Comput. Sci. 35 (2008) 15–23.

[3] Ismet Ozturk, Ibrahim Sogukpinar, Analysis and comparison of image encryption algorithm, Trans. Eng.Comput. Technol. 3 (2004) 38–42.

[4] Guodong Ye, Image scrambling encryption algorithm of pixel bit based on chaos map, Pattern Recognit. Lett 31 (2010) 347–354.

[5] Jui-Cheng Yen, Jiun-In Guo, A new chaotic key based design for image encryption and decryption, in: Proceedings of IEEE International Symposium on Circuits and Systems, vol. 4, 2000, pp. 49–52.

[6] Suk-Ling Li, Kai-Chi Leung, L.M. Cheng, Chi-Kwong Chan, Data hiding in images by adaptive LSB substitution based on the pixel-value differencing, in: Proceedings of the First International Conference on Innovative Computing, In-formation and Control, 2006, pp. 58–61.

[7] Shujiang Xu, Yinglong Wang, Jizhi Wang, Min Tian,Cryptanalysis of two chaotic image encryption schemesbased on permutation and XOR operations, in International Conference on Computational Intelligence and Security, 2008, pp.433–437.

[8] Rhouma Rhouma, Ercan Solak, Safya Belghith, Cryptanalysis of a new substitution– diffusion based image cipher, Commun. Nonlinear Sci. Numer. Simul.15 (7) (2010) 1887–1899.

[9] Jin-mei Liu, Qiang Qu, Cryptanalysis of a substitution-diffusion based image cipher using chaotic standard and logistic maps, in: Third International Sym-posium on Information Processing, 2010, pp. 67–69.

[10] Chengqing Li, Michael Z.Q. Chen, Kwok-Tung Lo, Breaking an image encryption algorithm based on chaos, Internat. J. Bifur. Chaos 21 (7) (2011) 2067– 2076.

[11] C.E. Shannon, "Communication theory of secrecy systems", Bell Syst. Tech. J. 28 (1949) 656–715.

[12] Alireza Jolfaei, Abdolrasoul Mirghadri, A new approach to measure quality of image encryption, Int. J. Comput. Sci. Netw. Secur. 2 (2010) 38–44.

[13] S.Vani Kumari,G.Neelima, "An Efficient Image Cryptographic Technique by Applying Chaotic Logistic Map and Arnold Cat Map",Volume 3, Issue 9, September 2013, International Journal of Advanced Research in Computer Science and Software Engineering pp.1210-1215

[14] Saranya Gokavarapu, S. Vani Kumari, "A Novel Encryption Using One Dimensional Chaotic Maps" Emerging ICT for Bridging the Future - Proceedings of the 49th Annual Convention of the Computer Society of India (CSI) Volume 1Advances in Intelligent Systems and Computing Volume 337, 2015, pp 193-203

