Securing Digital Image Using Cryptographic Key Generation Algorithm

V.ANUSUYA
(Department of CSE, National Engineering College, Kovilpatti)

M.PAPPA
(Department of CSE, National Engineering College, Kovilpatti)

Mrs.B.SHUNMUGA PRIYA
(Asst.Prof. Department of CSE, National Engineering College, Kovilpatti)

Abstract:

In the digital world, security is an important issue, and encryption is one of the ways to ensure security. This paper presents image encryption/decryption scheme using a password image. The proposed scheme is especially useful for encryption of large amounts of data, such as digital images using proposed key generation algorithm. This scheme satisfies the characters of convenient realization, less computation complexity and good security. The salient features of the proposed image encryption method are loss-less, cryptographic key encryption. The programming and simulation of the processes as well as the analysis of the results were done using MATLAB.

Keywords — **Block Cipher, Cryptography, Feistel Network, Image Decryption, Image Encryption.**

I. INTRODUCTION

Security is an important issue in communication and storage of images. Encryption/Decryption is one of the ways to ensure the security. Image security is the atmost concern as web attacks have become more and more serious. To make the data secure from various attacks and for the integrity of data we must encrypt the, military, financial institution, hospitals and private business deals with confidential images about their patient (in Hospitals), geographical areas (in research), enemy positions (in defense), product, financial status. Most of this information is now collected and stored on electronic computers and transmitted across network to other computer. If these confidential images about enemy positions, patient and geographical areas fall into the wrong hands, than such a breach of security could lead to declination of war, wrong treatment etc. Protecting confidential images is an ethical and legal requirement. Image encryption has applications in multimedia systems, medical imaging, telemedicine, and military communication. Many image content encryption algorithms have been proposed such as DES, 3DES, blowfish, AES, etc. Blowfish algorithm is highly secured because it has longer key length (more no of key size). The main aim behind the design of this proposal is to get the best security/performance trade off over existing ciphers. To achieve this result we are going to compare different parameters such as processing time, bandwidth, correlation, entropy etc of above mentioned algorithms.

II.LITERATURE SURVEY

Shahzad Alam, Amir Jamil, Ankur Saldhi, "Digital Image Authentication and Encryption Using Digital Signature",Computer Engineering And Applications(IAEA),2015 International Conference on Advances in,23 July 2015.

In this paper, a methodology for digital image authentication using digital signature is proposed. The hash of the original image is taken and is encrypted by RSA. The digital signature obtained is concealed in the image. Digital signature is sent along with the encrypted image which decreases the probability of meticulous attack by the intruder. The encrypted image is shuffled using Chaotic Logistic Map to get the final shuffled encrypted image. The use of Logistic Map improves the randomness in the image. For the authentication, a comparator is employed which evaluates correctness of the hash extracted. The simulations have been carried out to examine the proposed authentication and encryption technique.

Drawbacks:

The main disadvantage is Digital signatures, like all technological products, are highly dependent on the technology . In this era of fast technological advancements, many of these tech products have a short shelf life.

Tung-Shou Chen, Chin-Chen Chang, Min-Shiang Hwang, "A Virtual Image Cryptosystem Based Upon Vector Quantization" IEEE Transactions on Image Processing(volume: 7, Issue:10, oct 1998).

We propose a new image cryptosystem to protect image data. It encrypts the original image into another virtual image. Since both original and virtual images are significant, our new cryptosystem can confuse illegal users. Besides the camouflage, this new cryptosystem has three other benefits. First, our cryptosystem is secure even if the illegal users know that our virtual image is a camouflage. Second, this cryptosystem can compress image data. Finally, our method is more efficient than a method that encrypts the entire image directly.

Xin Zhang, Weibin Chen, "A New Chaotic Algorithm For Image Encryption", Audio, Language and Image Processing, 2008. ICALIP 2008. International Conference on 08 Aug 2008.

In this paper, a new image encryption algorithm is presented based on Henon chaotic maps in order to meet the requirements of the secure image transfer. There are several parameters in this kind of chaos system, and it is sensible to the original value and unpredictable. The results of several experimental, statistical analysis and key sensitivity tests show that the proposed image encryption scheme based on Henon chaotic maps provides an efficient and secure way for image encryption. The distribution of grey values of the encrypted image has a random-like behaviour.

Drawbacks:

The main drawback is that the time taken for encrypting image takes longer time so that the process gets delay.

Jinping Fan, Yonglin Zhang, "Color Image Encryption And Decryption Based on Double Random Phase Encoding Technique" Photonics and Optoelectronics,2009. SOPO 2009. Symposium on 01 sep 2009.

A new technique of color image encryption based on double random phase encoding technique is proposed. The color image to be encrypted is first separated into three color channels: red (R), green(G) and blue (B). Each of these channels is encrypted using double random phase encoding technique and then three new coding image matrixes are constructed. We choose a large enough absolute symmetric image as host image which also been segregated into tricolor channels to hide the real and imaginary parts of the encoding data and discuss the method how to construct the complete symmetrical host image. In the receipted side simple extracted and decryption operations can be employed to obtain the reconstructed image that is the same as the original image. Computer simulations were done in MATLAB and the result shows that the method is powerful for color image encryption and decryption.

Drawback:

We believe that it would be difficult to estimate the correct key image by employing the proposed method because the KPA using simulate d annealing also uses the amplitude of the encrypted image.

III. BLOWFISH ALGORITHM

Blowfish is a symmetric-key block cipher, designed in 1993 by Bruce Schneier and included in a large number of cipher suites and encryption products. Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date. Schneier designed Blowfish as a general-purpose algorithm, intended as an alternative to the aging DES and free of the problems and constraints associated with other algorithms. At the time Blowfish was released, many other designs were proprietary, encumbered by patents or were commercial or government secrets. Schneier has stated that, "Blowfish is unpatented, and will remain so in all countries. The algorithm is hereby placed in the public domain, and can be freely used by anyone."

Blowfish is a symmetric block cipher that can be effectively used for encryption and safeguarding of data. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data. Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms. Blowfish is unpatented and license-free, and is available free for all uses. Blowfish Algorithm is a Feistel Network, iterating a simple encryption function 16 times. The block size is 64 bits, and the key can be any length up to 448 bits. Although there is complex initialization phase required before any encryption can take place, the actual encryption of data is very efficient on large microprocessors.

A. Blowfish Encryption

In Fig.1. to the left shows Blowfish's encryption routine. Each line represents 32 bits. There are five subkey-arrays: one 18-entry P-array (denoted as K in the diagram, to avoid confusion with the Plaintext) and four 256-entry S-boxes (S0, S1, S2 and S3).

Every round *r* consists of 4 actions: First, XOR the left half (L) of the data with the *r* th P-array entry, second, use the XORed data as input for Blowfish's

F-function, third, XOR the F-function's output with the right half (R) of the data, and last, swap L and R.

Fig.1.Functional Diagram of Blowfish Algorithm

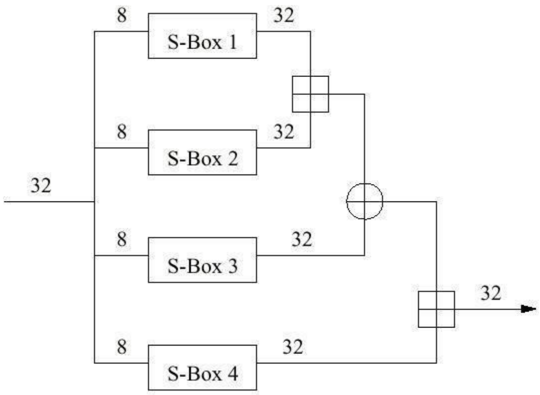
The F-function splits the 32-bit input into four eight-bit quarters, and uses the quarters as input to the S-boxes. The S-boxes accept 8-bit input and produce 32-bit output. The outputs are added modulo 2^{32} and XORed to produce the final 32-bit output (see image in the upper right corner).

After the 16th round, undo the last swap, and XOR L with K18 and R with K17 (output whitening).

B. Generating The Subkeys

Blowfish uses a large number of subkeys. These keys must be precomputed before any data encryption or decryption. The P-array consists of 18 32-bit subkeys: P1, P2… P18. There are also four 32-bit S-boxes with 256 entries each [5]:

S1, 0, S1, 1… S1, 255;



S2, 0, S2, 1… S2, 255;

The S-box and P-array generation process works as follow:

1. Initialize first the P-array and then the four S- boxes, in order, with a fixed string. This string consists of the hexadecimal digits of π:-

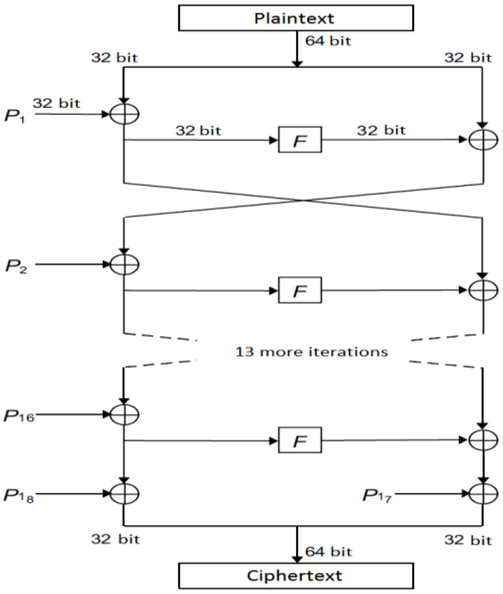
P1 =

0x243f6a88,

P2 =

0x85a308d3,

P3 = 0x13198a2e,



P4 = 0x03707344, etc.

2. XOR P1 with the first 32 bits of the key, XOR P2 with the second 32-bits of the key, and so on for all bits of the key (possibly up to P16). Repeatedly cycle through the key bits until the entire P-array has been XORed with key bits.

3. Encrypt the all-zero string with the Blowfish algorithm, using the subkeys.

4. Replace P1 and P2 with the output of step (3).

5. Encrypt the output of step (3) using the Blowfish algorithm with the modified subkeys.

6. Replace P3 and P4 with the output of step (5).

7. Continue the process, replacing all entries of the P-array, and then all four S-boxes in order, with the output of the continuously changing Blowfish algorithm.

Fig.2. S-Box In Blowfish Algorithm

In total, 521 iterations are required to generate all required subkeys.

C. Blowfish Decryption

Decryption is exactly the same as encryption, except that P1, P2, …, P18 are used in the reverse order. This is not so obvious because xor is commutative and associative. A common misconception is to use inverse order of encryption as decryption algorithm (i.e. first XORing P17 and P18 to the cipher text block, then using the P-entries in reverse order).

IV. PROPOSED SYSTEM

In this proposed model, image security has been obtained by encrypting and decrypting image using cryptography. The proposed method called "Enhanced Blowfish Algorithm for Image Encryption & Decryption with Supplementary Key" is an encryption and decryption technique. It is based on Blow Fish algorithm with additional secret key to provide extra security while sending and receiving images and sensitive data.

An image is given as input. Another image is selected as password image. From the password image, a key is generated. The original image is encrypted using the key. The image so obtained is the Encrypted image. The encrypted image is treated as input .Again the password image is selected and key is generated. Using the key, the encrypted image is decrypted. The original image is obtained. Blowfish algorithm is a fast and alternative to existing encryption algorithms. It is called as symmetric block chipper to safeguard the data effectively.

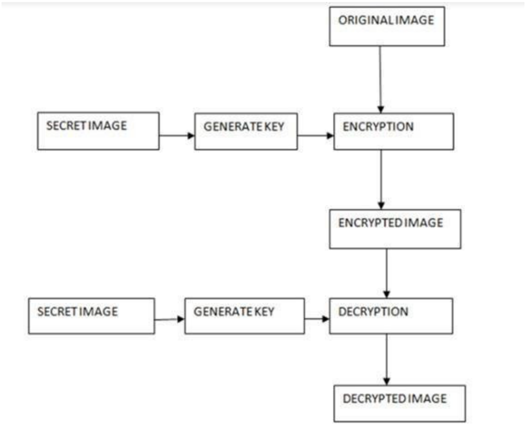


Fig.3.Proposed system diagram

PROPOSED KEY GENERATION

An image is divided into number of pixels .RGB value for each pixel is calculated .From the RGB values, its binary equivalent is calculated. Binary values are converted to its decimal values. Based on the total number of pixels, the decimal values are grouped.RMS values for each group is calculated ASCII values for each RMS value is calculated and the password is generated. From this password, the key is generated using the Blowfish Algorithm.

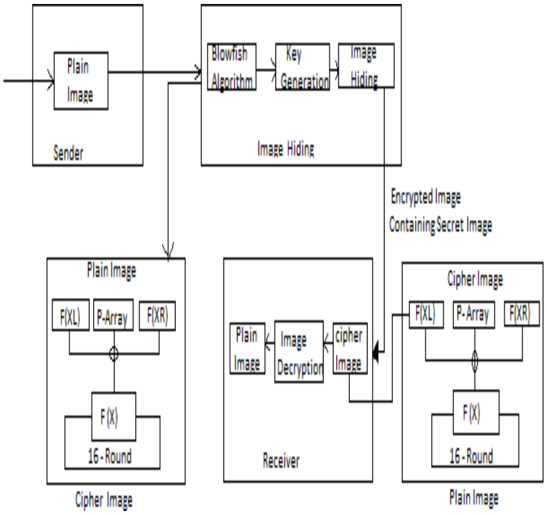


Fig.4. Architectural Diagram

A. Proposed Encryption Algorithm based on Blowfish: .

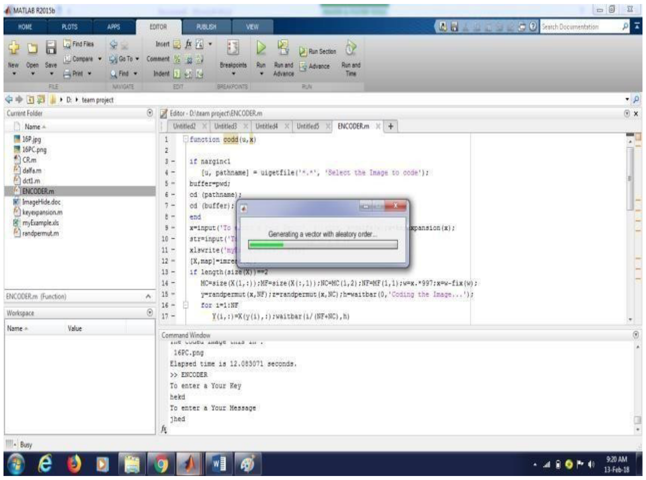
Step 1: Initialize S Box and T Box as arrays.
Step 2: Convert the matrix Inverse to Transpose and store in T Box.
Step 3: The input is a 64-bit data element, x.
Step 4: Divide x into two 32-bit halves: xL, xR.
Then, for i = 1 to 16: xL = xL XOR Pi xR =

F(xL)XOR xR Swap xL and xR After the sixteenth round, swap xL and xR again to undo the last swap. Step 5: Then, xR = xR XOR P17 and xL = xL XOR P18.
Step 6: Finally, recombine xL and xR to get the cipher image.

B.Image Decryption with the Secret Key Decryption

Step 1: Initialize S Box and T Box as arrays.
Step 2: Secret key comparison between original key which is created while encryption.
Step 3: The input is a 64-bit data element, x. Step 4: Divide x into two 32-bit halves: xL, xR.
Then, for i = 1 to 16: xL = xL XOR Pi xR = F(xL)XOR xR Swap xL and xR After the sixteenth round, swap xL and xR again to undo the last swap.
Step 5: Then, xR = xR XOR P17 and xL = xL XOR P18.
Step 6: Finally, recombine xL and xR to get the original image.

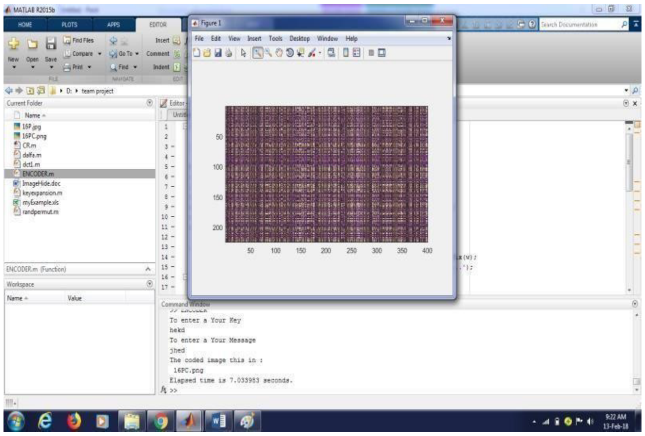
V.EXPERIMENTAL RESULT:



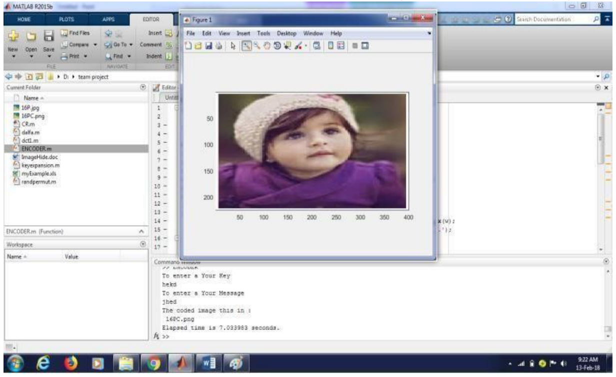
```
function codd(u,x)

if nargin<1
   [u, pathname] = uigetfile('*.*', 'Select the Image to code');
buffer=pwd;
cd (pathname);
cd (buffer);
end
x=input('To                                          xpansion(x);
str=input('T
xlswrite('my
[X,map]=imre
if length(size(X))==2
   MC=size(X(1,:));MF=size(X(:,1));NC=MC(1,2);NF=MF(1,1);w=x.*997;x=w-fix(w);
   y=randpermut(x,NF);z=randpermut(x,NC);h=waitbar(0,'Coding the Image...');
   for i=1:NF
      Y(i,:)=X(y(i),:);waitbar(i/(NF+NC),h)
```

```
 16PC.png
Elapsed time is 12.083071 seconds.
>> ENCODER
To enter a Your Key
hekd
To enter a Your Message
jhed
```



```
To enter a Your Key
hekd
To enter a Your Message
jhed
The coded image this in :
 16PC.png
Elapsed time is 7.033983 seconds.
>>
```



```
>> ENCODER
To enter a Your Key
hekd
To enter a Your Message
jhed
The coded image this in :
 16PC.png
Elapsed time is 7.033983 seconds.
>>
```

VI. CONCLUSION

An encryption algorithm has been designed and developed using blowfish with key in MATLAB. Various images are used in experiments and performance measures are recorded. In addition to that security factor is also analyzed.

VII. REFERENCES

1] T Nie and T Zhang. "A study of DES and Blowfish encryption algorithm." TENCON 2009 IEEE Region 10 Conference. pp 1-4, January 2009

2] D.Zhang, W.K. Kong, J. You, M. Wong, "On-line palmprint identification", IEEE Trans. Patt. Anal. Mach. Intell. 25 (2003) 1041-1050.

3] SyedAliNaqiGilani, M. Ajmal Bangash "Enhanced block based color image encryption technique with confusion" in the Proceedings of the 12th IEEE International Multi topic Conference,

4] M Salleh, S Ibrahim, IF Isnin, "Image encryption algorithm based on Chaotic Mapping" Journal Teknologi, University Teknologi of Malaysia,

5] KedeMa, Weiming Zhang, Xianfeng Zhao, Member, IEEE, NenghaiYu, and Fenghua Li"Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption" ieeetransactions on information.

6] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized- LSB data embedding,"

7] IEEE Trans. Image Process., vol. 14, no. 2, pp. 253–266, Feb. 2005.

8] Pia Singh Prof. Karamjeet Singh "Image encryption and decryption using blowfish algorithm in matlab" International Journal of Scientific & Engineering Research, Volume 4,Issue 7, July-2013 150 ISSN 2229-5518.

9] M. Alattar, "Reversible watermark using the difference expansion of a generalized integer transform," IEEE Trans. Image Process., vol. 13, no. 8, pp. 1147–1156, Aug. 2004.
AshakAlabaichi, FaudziaAhmad, RamlanMamod "Security Analysis of Blowfish Algorithm", 2013 IEEE.

10] Russell K. Meyers and Ahmed H. Desoky "An Implementation of the Blowfish Cryptosystem", 2008 IEEE.