A New Image Encryption Algorithm Based Slicing and Displacement Followed By Symmetric and Asymmetric Cryptography Technique

Ankita Maheshwari
M.E Scholar JIT Khargon, amaheshwari44@gmail.com

Abstract: This paper titled "A New Algorithm for Image Encryption Based on Slicing, Displacement Followed by Symmetric Encryption" is proposed for image encryption by studding the principle of the image encryption algorithm. In this, a new hybrid image encryption algorithm is proposed by analyzing the principle of the encryption algorithm based on the combination of symmetric and asymmetric encryption. The experimental results based on combination of symmetric and asymmetric encryption will approve the effectiveness of the proposed concept, and the combination of symmetric and asymmetric encryption will show large variation in key space and provide high-level security. Proposed algorithm will support to integrity, authorization, accuracy of images which is transmitting in public network. As we know that, an image-based data requires more effort during encryption and decryption. This research introduces a block-based algorithm which is the combination of "Slicing and Displacement of RGB value of a Pixel" and "Block Cipher" base image encryption algorithm. The original image was divided into four equal parts, where each part of image will rearranged into displacement of RGB value of a pixel and then resultant image will divided into pixel blocks. Read binary value of pixel blocks. This binary value will be process by encryption process through binary value of selected key. Now finally encrypted image will be produced. This process will repeat on each parts of image. After that each part will be combining and produce final cipher image. Encryption key will also encrypted by asymmetric key concept so key exchanging problem will not occur in this system. The Proposed Architecture for encryption and decryption of an image using suitable user-defined key is developed. The cipher image generated by this method can be very in size as the original image due to image scaling to make 128 bits block at a time and is suitable for practical use in the secure transmission of confidential information over the Internet.

Keyword: *Encryption, Decryption, Security, Image, Cryptography, Pixel.*

*****

I. INTRODUCTION

The concept of image encryption and the word cryptography might be intimidating and complicated. The objective of the report is to develop a software tool that helps the user and the operations to achieve images security. A platform independent tool with user-friendly graphical user interface, using already existing techniques and algorithms for cryptographic operations will be resulting product. Nowadays, information security is becoming more important in data storage and transmission. Images are widely used in several processes. Therefore, the protection of image data from unauthorized access is important. Image encryption plays a significant role in the field of information hiding. Image hiding or encrypting methods and algorithms range from simple spatial domain methods to more complicated and reliable frequency domain ones. Most of the available encryption algorithms are mainly used for textual data and may not be suitable for multimedia data such as images. "A New Algorithm for Image Encryption Based Slicing, Displacement Followed by Symmetric Encryption" is a block cipher algorithm. Proposed algorithm is the improvement of existing algorithm. The proposed research resolving and improving security issue of existing algorithm and improving overall efficiency by adding more confusion with the help of proposed encryption algorithm thus resulting in a strong cryptographic algorithm. In this research Histogram, entropy and correlation are the measurement and analyzing parameter of existing and proposed algorithm and ensuring that encrypted entropy and correlation should be good during comparison form existing algorithm. The simple architecture in the figure below shows the process of encryption and decryption. Figure 1 is showing the general architecture of the proposed encryption process where an image will select as an input then slicing function will slice image into four equal parts, after that each part will pass from displacement process finally displaced part will be process with proposed encryption algorithm with 128 bits size key value then proposed encryption process will execute number of operation then each encrypted parts of image will be once again combine through combine process and finally a cipher image will produced as an output

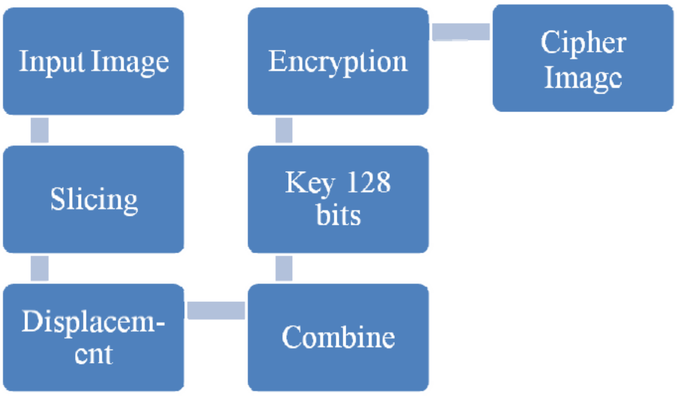


Figure1: Architecture Diagram for Encryption

Figure 2 is showing the simple architecture of the proposed decryption process where a cipher an image will select as an input then slicing function will slice image into four equal parts then proposed decryption process will execute number of operation with 128 bits size key value. After that each decrypted parts of image will be redisplayed vertically then each parts of image will once again combine and finally a original image will produced as an output

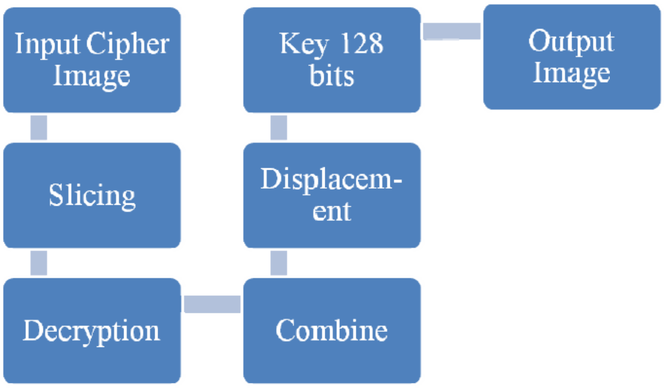


Figure2: Architecture Diagram for Decryption

II. PROPOSED WORK

In most of the natural images, the values of the neighboring pixels are strongly correlated (i.e. the value of any given pixel can be reasonably predicted from the values of its neighbors). In order to dissipate the high correlation among pixels and increase the entropy value, I propose a newly design image encryption algorithm that divides the image into blocks and then shuffles their positions before it passes them to the proposed encryption algorithm. By using the correlation and entropy as a measure of security, this process results in a lower correlation and a higher entropy value when compared to using the proposed algorithm alone, and thus improving the security level of the encrypted images. There are two main keys to increase the entropy; the variable secret key of the displacement process (horizontal and Vertical) and the variable secret key of the proposed encryption algorithm. The variable secret key of the displacement process determines the constant, which is used to build the secret image with a variable number of blocks. If the key is changed, another constant will be generated, and then a different secret image is obtained. The variable secret key of the proposed encryption algorithm is used to encrypt the displaced image. This encryption process decreases the mutual information among the encrypted image variables (i.e. high contrast) and thus increasing the entropy value. In this paper I proposed newly design block-based encryption algorithm where block diagram of proposed system shown in figure 3, in order to increase the security level of the encrypted images.

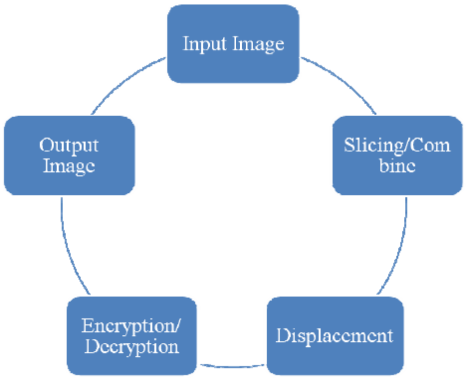
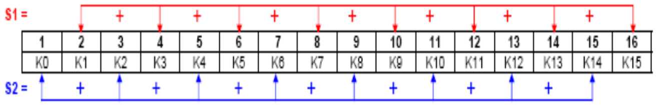


Figure 3: Block Diagram of Proposed System

Slicing Approach: Here we are slicing process as 4 for the purpose of simulation, high performance and easier understandability in the concept. Once the slices are update with its new positions. We follow next step. To slicing an image we have used simple concept like select initial X, Y coordinate, maximum X, Y coordinate and intermediate X, Y Coordinate apply mathematic function.

Displacement Approach: In the First step original image is sliced and divided into 4 sub slice. This sliced sub image is now used for displacement. Here we are using two displacement approaches (vertical and horizontal) one by one. This displace of pixel position of sub image reduces the correlation between the adjacent pixels and it may be causes of higher entropy. This approach is being tested by making pixel blocks of different sizes and then their result is being analyzed. For vertical and horizontal displacement of pixel position we have used number of vertical pixel blocks in sub image and accordingly it will explosively displace the pixel blocks in vertical direction in the 1:1 manner; according to this method, block at location 1st will to 2nd block position, 2nd block will move to 3th block position and 3rd block will move to 4th block position. Similarly block at location 4th will to 3rd block position, 3rd block will move to 2nd block position and 2nd block will move to 1st block position. Similarly same process will apply on horizontal displacement approach. This process will apply on each sub part of image.

Proposed Encryption Algorithm: Byte Array containing 16 characters (bytes) long key



1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
K0	K1	K2	K3	K4	K5	K6	K7	K8	K9	K10	K11	K12	K13	K14	K15

Ki denotes ith index in 16 byte long key array

Calculations:

Encryption Side

S1 = (K1×2) + (K3×4) + (K5×6) + (K7×8) + (K9×10) + (K11×12) + (K13×14) + (K15×16)

$S2 = (K0\times1) + (K2\times3) + (K4\times5) + (K6\times7) + (K8\times9) + (K10\times11) + (K12\times13) + (K14\times15)$

Sum = absolute value of (S1+S2)

Compulsory Condition: Value of Sum must always contain exactly three digits e.g. *103,387* etc.

Case-1: if $Sum<100$ then error message is displayed that the key is too weak.

Case-2: if $100\leq Sum\leq 999$ then it satisfies the condition and therefore further processing takes place as follow:

Step-1: Let $Sum = d_1d_2d_3$, then *RGB* values of all the four pixels (P_1, P_2, P_3 and P_4) are modified as follow:

Perform d1 number of right shifts in R byte of all four pixels
Perform d2 number of right shifts in G byte of all four pixels
Perform d3 number of right shifts in B byte of all four pixels

Step-2:

If d1 is an odd number
Reverse the bits in P_1
Else Perform EXOR operation between P_1 and K_1
If d_2 *is an odd number*
Reverse the bits in P_2
Else Perform EXOR operation between P_2 and K_2
If d_3 *is an odd number*
Reverse the bits in P3
Else Perform EXOR operation between P3 and K3
If d_4 *is an odd number*
Reverse the bits in P4
Else Perform EXOR operation between P4 and K4

Case-3: if $Sum>999$ (i.e. Sum contains more than three digits) then only last three least significant digits are considered and the most significant digit is ignored. It is because most significant (left most) digit has the least possibility of getting changed whereas as we move towards right, digits change rapidly, which is good for encryption process.

Example: Let $Sum = d_1d_2d_3d_4$

Then only d_2, d_3 and d_4 will be considered according to step-2 and d_1 will be ignored as the probability of this digit to change is least among d_1, d_2, d_3 and d_4.

REVERSE PROCESSING IS DONE ON DECRYPTION SIDE i.e. firstly step-2 and then step-1 is carried out

Handel Key Exchange Issue: Proposed research is the designing and implementation of a new Hybrid Image encryption algorithm. Proposed technique is a method of image encryption that combines two or more encryption technique and usually includes a combination of symmetric and asymmetric (public-key) encryption to take benefit of the strengths of each type of encryption. Symmetric encryption has the performance advantage and therefore is the common solution for encrypting and decrypting performance-sensitive data. However, symmetric encryption has a downside the cryptographic key needs to be known to both the sender and receiver of encrypted data, and the exchanging of the key over an insecure channel may cause security risks. On the other hand, asymmetric or public-key encryption provides better security in that the cryptographic key required for decrypting data does not have to be shared with other parties. This is more secure, but it comes with a price the computation speed is slower than in the case of symmetric encryption. A solution to this problem is to first encrypt and exchange the symmetric encryption key by means of asymmetric encryption, and then use that symmetric key for encrypting and decrypting the actual data. Although this method provides protection while the encrypted key is transferred between parties, it is not necessarily secure at the moment when the encrypted symmetric key is being decrypted. If an adversary is monitoring the system where this takes place and if the system is not white-box protected, the cryptographic keys can be extracted in plain form. For asymmetric key algorithm I will use simple RSA algorithm. Figure 4 is showing the proposed crypto system to encrypt/ decrypt an image.

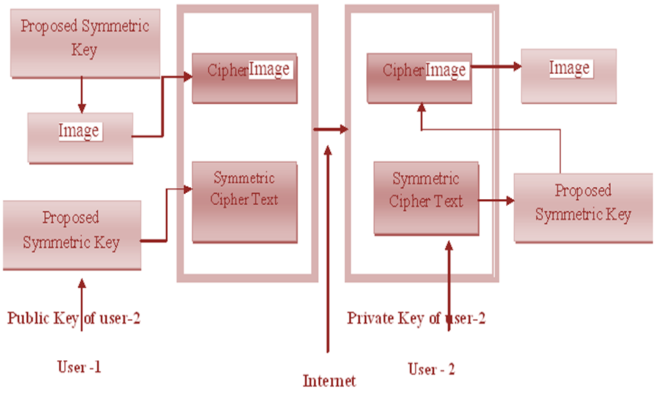


Figure 4: Proposed Crypto System for Image Encryption/Decryption

III. RESULTS ANALYSIS

Here we are presenting the experiment results based on selected parameters. All the results are approximately calculated and best of our knowledge it can be vary on environment condition because its machine oriented. Key length is the important factor of the proposed concept which is distingue from existing concept which is defined in [18, 19]. Security is the primary task of the proposed concept. Key exchanging is also important issues in the symmetric key concept so we have used asymmetric key (RSA) in the proposed concept. The presented experimental results show the superiority of the proposed concept as compare existing concept in terms of the entropy, and correlation. At run time we have used following machine configuration (See table 1)

Table 1: System Configuration

Items	Description
Processor	Intel Pentium Dual Core 1.5 GHz.
Memory	1 GB
HDD	20 GB
Software Application	JDK 1.6
Database	MS-Access

Selected parameter is entropy, correlation and histogram of the image which is describe below.

- Entropy:

$$H_e = -\sum_{k=0}^{G-1} P(k)\log_2(P(k))$$

Where:
He: entropy.
G: gray value of input image (0... 255).
P(k): is the probability of the occurrence of symbol *k*.

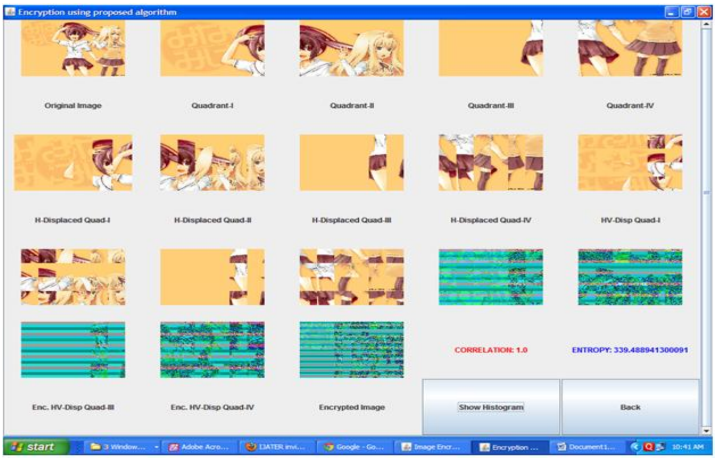
- Correlation:

$$r = \frac{n\sum(xy)-\sum x\sum y}{\sqrt{[n\sum(x^2)-(\sum x)^2][n\sum(y^2)-(\sum y)^2]}}$$

Where
r: correlation value
n: the number of pairs of data
∑*xy*: sum of the products of paired data
∑*x*: sum of *x* data
∑*y*: sum of *y* data
$\sum x^2$: sum of squared *x* data
$\sum y^2$: sum of squared *y* data

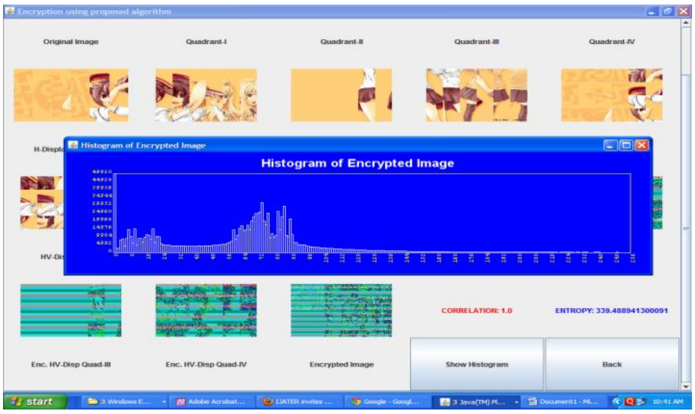
Snap Shot of Results:

Proposed Concept



CORRELATION: 1.0
ENTROPY: 339.488941300091

Figure 5: Encrypted Image Snap Shot



CORRELATION: 1.0
ENTROPY: 339.488941300091

Figure 6: Histogram of Image Snap Shot

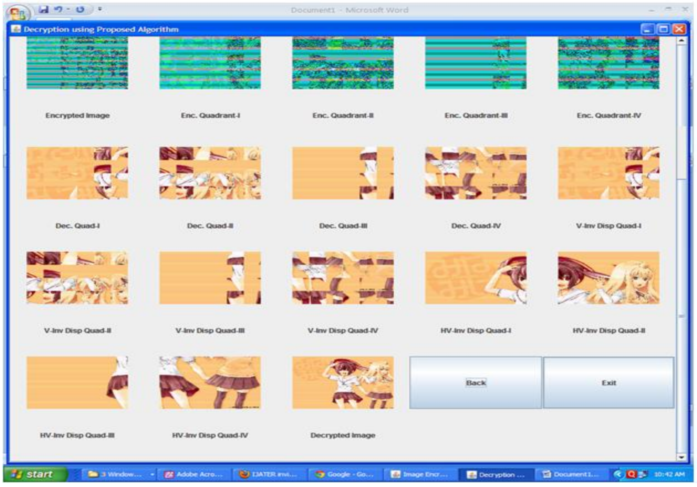


Figure 7: Decrypted Image Snap Shot

The Snap shot form 5. To 7, showing the encryption, histogram and decryption of selected images by proposed concept. All the results are based on our knowledge and approximate. It can be vary on different environment. The proposed system is encrypting and decrypting an image and correspondingly showing entropy and correlation. The proposed system has run number of times approximately to calculate results and every time same images are respectively encrypted by existing concept and "Proposed concept" by copying them. Size of the selected key was same in each time. Finally, the outputs of the comparison system are entropy and correlation which is noted in numeric form and it's shown in table 2.

Table 2: Results Comparisons

S.NO	Images	Name of Concept	Entropy	Correlation
Approx Results				
1	Imag1.jpg(1024X 781)	Proposed Concept	314.277	1.0
2	Imag2.jpg(1280X 1024)	Proposed Concept	339.488	1.0

From figure 5 to 7 and table 2 we have analyzed that entropy of the encrypted image Imag1 of size 1024*781 is 314.277 with correlation value 1.0 and Imag2 of size 1280*1024 is 339.488 with correlation value 1.0. From these results we can conclude that correlation value producing same results for both but entropy value is producing different value. Larger image size will produce large entropy value which good for security.

IV. Conclusion

Conclusion: In this paper a simple and strong concept has been proposed for image security using a new technique based on the slicing of the image into sub parts and displacement of pixel position of each sub part and a new developed symmetric encryption algorithm with the asymmetric key concept. From the proposed concept we are looking that the correlation are vary from image to image. In this paper we have selected two images for results purpose but coincidently both are producing same correlation in all three concepts. But it's clearly defined from entropy that proposed concept is producing good results. Following are certain limitation in the proposed algorithm. Java Virtual Machine framework should be installed at user end to access this application. It would encrypt only limited type of images because proposed algorithm is built for only one or two type of images. In future we will try to improve security level of the proposed algorithm. It will also try to resolve limitation of image type that mean any type of image will be encrypt and decrypt through proposed algorithm Further development of the algorithm to accommodate tighter generic security reductions for image encryption is therefore desirable.

References

[1] Bruce Shnier "Applied Cryptography Second Edition Protocols. Algorithms, and Source, and Source Code in C", John Wiley and Sons, Inc., 1996.

[2] B. Schneier, Applied Cryptography, John Wiley & Sons, New York, 1994.

[3] B. Schneier, "Data Guardians," MacWorld, Feb 1993, 145-151.

[4] Onwutalobi Anthony-Claret *"Using Encryption Technique"* Department of Computer Science,University of Wollongong Australia, Anthony.claret@ieee.org

[5] William stallings, *"Cryptography and Network Security:Principles & Practices"*, second edition.

[6] 16 S. Changgui, B. Bharat, "An efficient MPEG video encryption a lgor i thm, " *Proc e edings of the symposium on reliable distributed systems, IEEE computer society Press*, 1998, pp. 381-386.

[7] Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda, Image Encryption Using Advanced Hill Cipher Algorithm, International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009

[8] Zhang Yun-peng, Liu Wei, Cao Shui-ping, Zhai Zheng-jun, Nie Xuan , Dai Wei-di, Digital image encryption algorithm based on chaos and improved DES, IEEE International Conference on Systems, Man and Cybernetics, 2009.

[9] Seyed Mohammad Seyedzade, Reza Ebrahimi Atani and Sattar Mirzakuchaki, A Novel Image Encryption Algorithm Based on Hash Function 6th Iranian Conference on Machine Vision and Image Processing, 2010.

[10] Ismail Amr Ismail, Mohammed Amin, Hossam Diab A Digital Image Encryption Algorithm Based a Composition of Two Chaotic Logistic Maps , International Journal of Network Security, Vol.11, No.1, PP.1 -10, July 2010.

[11] Kamali, S.H., Shakerian, R., Hedayati, M.,Rahmani, M., A new modified version of Advance Encryption Standard based algorithm for image encryption,Electronics and Information Engineering (ICEIE), 2010 International Conference.

[12] Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh, Sushanta Biswas, D. Sarkar Partha Pratim Sarkar, Image Encryption Using Affine Transform and XOR Operation ,International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN 2011).

[13] Sesha Pallavi Indrakanti , P.S.Avadhani, Permutation based Image Encryption Technique, International Journal of Computer Applications (0975 – 8887) Volume 28– No.8, 2011.

[14] Qais H. Alsafasfeh , Aouda A. Arfoa, Image Encryption Based on the General Approach for Multiple Chaotic Systems Journal of Signal and Information Processing, 2011.

[15] Ibrahim S I Abuhaiba , Maaly A S Hassan, Image Encryption Using Differential Evolution Approach In Frequency Domain

[16] Revised for accepted but unpublished paper of min Different Techniques of Image encryption : A literature Review at IJETAE

[17] Fews texts taken as reference from the papers : http://www.waset.org/journals/waset/v3/v3-7.pdf
Analysis and Comparison of Image Encryption Algorithms by Ismet Öztürk and Ibrahim Soukpinar , Image Using Different Technique A Review: Komal D Patel, Sonal Belani (ISSN 2250-2459, Volume 1, Issue 1, November 2011) and http://www.ijest.info/docs/IJEST10-02-06-142.pdfThey are in edited language and I give thanks to those writers.

[18] Amnesh Goel, Reji Mathews, Nidhi Chandra "Image Encryption based on Inter Pixel Displacement of RGB Values inside Custom Slices" International Journal of Computer Applications (0975 – 8887) Volume 36– No.3, December 2011.

[19] Amnesh Goel and Nidhi Chandra "A Technique for Image Encryption Based On Explosive n*n Block Displacement Followed By Inter-Pixel Displacement of RGB Attribute of A Pixel" 2012 International

Conference on Communication Systems and Network Technologies

[20] Jose J Tharayil, E.S. Karthik Kumar, Neena Susan Alex “Visual Cryptography Using Hybrid Halftoning and Inter-Pixel Exchanging” 2012 IEEE Students’ Conference on Electrical, Electronics and Computer Science”

[21] Rithmi Mitter and M. Sridevi Sathya Priya “a highly secure cryptosystem for image encryption” IEEE Conferences 2012

[22]] Arun Raj R, Sudhish N George and Deepthi P. P. “An Expeditious Chaos Based Digital Image Encryption Algorithm” 1st Int’l Conf. on Recent Advances in Information Technology | RAIT-2012.