Enhanced Efficient & Secure Steganography Algorithm with low distortion

Priyanka Singh[1], Garbita Gupta[2]

[1]Priyanka Singh, Dept.of CSE, BIST, MP, India
[2]Prof.Garbita Gupta, Dept.of CSE, BIST, MP, India

---***---

Abstract - *Information security is prime focus now a day's in a digital life. Many times there is a need to store or share our secret information over unsecure network. There is always a fear that our information should be stolen In such situation, to secure our information many security algorithms have been designed. Here, security implies confidentiality, authenticity and integrity. The scope of this paper is limited to confidentiality only. There are number of confidentiality algorithms exist but the question is whether they are enough strong according to the needs of today and the answer is no, all the algorithms in existence are efficient in only some parameters and are compromising with the other parameters. The research in this paper has taken an aim to design a new algorithm that ensures complete confidentiality without compromising on other parameters. This paper has proposed a hybrid algorithm that is a combination of encryption/decryption algorithm, lossless data compression algorithm and steganography algorithm. Implementation result proves the success of this algorithm by showing its efficiency against the existing algorithm.*

Key words: Computer Security, Steganography, MSA Algorithm, Encryption Decryption Algorithm.

1. INTRODUCTION

Security of information is very important in today's life. In digital era, everyone used to keep their data on digital network and access them whenever needed. Many of that information are very special and secret that does not want to be share with everyone or want to share it with the limited people. It requires security to keep our secret data safe and away from the intruders. Here, Security implies: Confidentiality, Authenticity and Integrity. Confidentiality means to ensure that unauthorized person cannot read the information. Authentication means to ensure that communication can be done by only authorized person and Integrity ensure that receiver received the same copy transmitted or stored by the sender. This paper keeps their scope limited to confidentiality only.

To ensure the confidentiality many different types of algorithm have been designed. Cryptographic encryption/decryption and steganography both types of algorithm are used to ensure confidentiality. Encryption/ Decryption is a process to shuffle the arrangement of characters or replaced or manipulate the characters in such a way that no one can understand the true meaning of secret text. This process is called encryption while regenerate the data in their original form is called decryption. The process of encryption or decryption is done on the basis of key which can be symmetric or asymmetric at both ends. AES and DES are the most popular encryption/decryption algorithms.

Steganography on the other end work on some other principle. It hides the secret information behind any media file in such a way that no one can guess the presence of secret information. This media file can be any text file, image file or audio/ video file. LSB method is the most popular method used for steganography.

As to ensure the confidentiality already lots of algorithm are in existence but still there are some fight running on to design an algorithm which are more powerful and efficient compare to all existing algorithms. The problem with the existing algorithms is all have their merits and demerits. In order to improve one factor (parameter) algorithms are compromising with the other parameters.

Today, time are changing very rapidly, we have come to the time of micro computers from the time of big and limited computers. Requirements are changed, speed and security matters.
The objective of this paper is to study all such algorithms and design an algorithm that are efficient and secure as compared to the existing one.

2. LITERATURE SURVEY

As discussed in SECTION I, AES and DES are the standard encryption/ decryption algorithms used to ensure the confidentiality and LSB is used in steganography algorithm. In order to design better algorithm than the existing algorithms, a research was published in 2016, with a title "A Hybrid Approach of Image Steganography". This research is a fusion of both encryption/decryption and steganography algorithm. It first encrypt the secret data using Key Pixel Cipher approach and then the resultant cipher compressed using LZW compression method and finally hides the resultant behind the image using modified LSB method. In this, it hides the data in the upper LSB bit only when its adjacent LSB bit of all the pixel have conceived a bit of secret data for better quality of the stego-image.

Algorithm proposed in paper [2] is again a fusion of encryption/decryption algorithm and image steganography based on modified Data Encryption Standard (DES). It takes an advantage of S-Box mapping used in DES. It first, encrypt the data using modified DES algorithm which uses two key of size eight bits and then it hide the cipher text generated by modified DES into cover image file. Steganography algorithm proposed in this paper uses simple LSB method which hides 2 bits of cipher text behind each pixel of image. The problem identified by this dissertation is in its key size. It uses two key of eight bit which is very weak. It requires only 216 (i.e. 65536) combination to guess the key, this value can be easily solved by computer. Also after implementing this paper it is found that there is a chance of improvement in timing and distortion in cover file.

In [4] a new steganography method is proposed which is again a combination of encryption/ decryption algorithm and steganography algorithm. This paper presents a technique for Image steganography based on LSB using X-box mapping where they have used several X boxes having unique data. Hiding of a secret information is done by Steganography algorithm where they use four different unique X-boxes with sixteen values (represented by 4-bits) and each value is mapped with the four LSBs of the cover image. This mapping provides enough safety and security to the payload because without having the knowledge of mapping rules no one can extract the secret data.

In [5], the paper focuses on again combination of two algorithms encryption/ decryption algorithm and steganography algorithm. This paper proposed a new technique called Metamorphic Cryptography. The secret information is transformed into a cipher image using a key, concealed into another image using Steganography by converting it into an intermediate text and finally transformed once again into an image. The problem detected by this dissertation is that the algorithm uses minimum size of cover file but at the cost of distortion. The algorithm proposed in this paper has high distortion.

In [6], A new symmetric key cryptographic algorithm is introduced named DJMNA. Modified Generalized Vernam Cipher (MGVC) method and DJSA method are the two methods used in the algorithm. The Generalized Vernam Cipher algorithm extends message encryption to any type of data encryption. This is done by using ASCII code of all characters (0-255). This makes the encryption process very hard to decrypt by using any brute force method. The problem detected in this paper is its timing. It is found after implementation that it has high avalanche effect but it is worst to use for a large file. It is not a time efficient algorithm.

In [7], again a new cryptographic algorithm is proposed named BEST, the key feature of this proposed algorithm is its time efficiency also it uses 10 random keys to encrypt the plaintext into cipher text. But the problem detected in this paper is its avalanche effect which is very low. Also the algorithm needed a common database that shares between both the parties (sender and receiver) which is used to store the random secret key. If intruders gain to get access on this database than the whole security is for no use. Also maintaining and managing database makes this algorithm less preferable.

In [8] a new cryptographic algorithm is proposed named NJJSAA. It is a symmetric key encryption/ decryption algorithm also it has high avalanche effect but again it is not a time efficient algorithm. The key feature of this algorithm is its key which is totally randomized. Also it has large key size which is not easy to guess.

In [9] a new technique for image steganography based on Huffman Encoding is proposed. In this two 8 bit gray level image of dimention M X N and P X Q are using as a image cover file and secret image respectively. Huffman Encoding is applying over the secret image/message before embedding and each bit of Huffman code of secret image embedded inside the image cover file by altering the least significant bit (LSB) of each of the pixel's intensities of cover image. The size of the Huffman encoded bit stream and Huffman Table are also embedding inside the cover image, so that the Stego-Image becomes standalone information to the receiver.

3. PROPOSED ALGORITHM

As discussed in the previous section, there are various algorithms in existence to ensure the confidentiality over data that stored or transmitted through networks. The problem identified in these algorithms is that they are efficient in only some parameters and compromising the efficiency on other parameters. In order to get the best solution for the above discussed problem this paper has proposed a novel algorithm which is actually a combination of proposed encryption/decryption algorithm, LZW compression technique and proposed steganography algorithm. The proposed algorithm is designed in such a way that it would be light weighted, efficient and secure so that it can be used anywhere in any network like wired, wireless or ad-hoc network.

Proposed encryption/decryption algorithm is a symmetric block cipher algorithm. The strength of a proposed encryption/ decryption algorithm is the concept of pseudo random number used in the algorithm. Block diagram of proposed encryption algorithm is shown in Figure 1, 2 & 3.
Steps of proposed encryption algorithm are:

1. First a key of length 126 bits and a secret text taken as an input.
2. Next calculate pseudo random number by adding all the 1's of a binary key.
3. Now, Generate three different keys of length 126 bits by using following rules:

a. If pseudo random number is even then keys will be:

   i. Key1 = XOR all bits of key by bit at pseudo random number position + 2 respectively
   ii. Key2 = XOR Key1 with input key
   iii. Key3 = Left circular rotation of Key2 by 2 bits

b. If pseudo random number is even then keys will be:

   i. Key1 = XOR all bits of key by bit at pseudo random number position + 1 respectively
   ii. Key2 = Left circular rotation of Key1 by 2 bits
   iii. Key3 = XOR Key1 with input key

4. Now, shuffle the according to the following schedule

a. If the remainder comes out 1 by dividing pseudo random number by 4

   i. Key1 = Key2
   ii. Key2 = Key3
   iii. Key3 = Key1

b. If the remainder comes out 2 by dividing pseudo random number by 4

   i. Key1 = Key3
   ii. Key3 = Key2
   iii. Key2 = Key1

c. If the remainder comes out 2 by dividing pseudo random number by 4

   i. Key1 = Key1
   ii. Key2 = Key3
   iii. Key3 = Key2

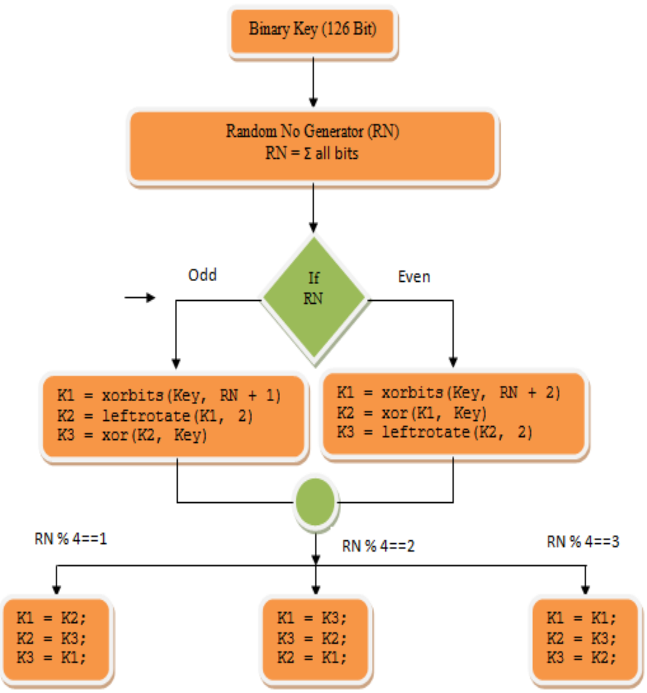

Figure -1: Random key generation of proposed algorithm

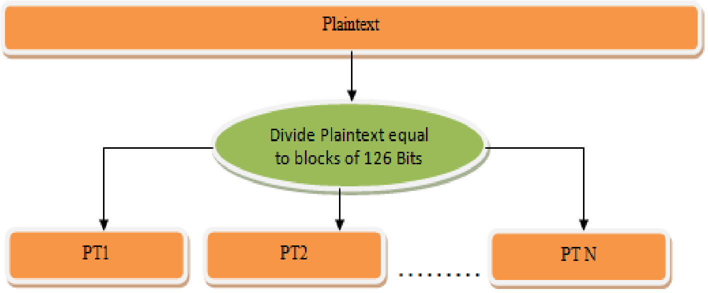

Figure -2: Preparation of Plain Text Chunks

5. Now, convert the secret text into 7 bit binary format & then divide it equal to chunks of 126 bits, if the last chunk has less bits than 126 bits then convert all the three keys of chunk length by just elemineting the last bits (Keys transformation will be done only when last chunk under process).
6. Next, repeat the following operations for each chunk:

a. Set PT = XOR Secret Text with Key1
b. PT = Circular Left Rotation of PT by RN bits
c. PT = XOR Secret Text with Key2
d. PT = Circular Left Rotation of PT by remainder of pseudo random number divided by 4.

e. Divide PT in two parts and swap them
f. PT = XOR all bits by bit at position pseudo random number.
g. PT = XOR Secret Text with Key3
h. PT = XOR all bits by bit at position remainder of pseudo random number divided by 4.
i. Result is Cipher Text of input chunk
j. Convert the resultant cipher text in to 8 bit character format

7. Exit of proposed encryption algorithm.

Now the data is compressed with the help of LZW compression technique.

Lastly, compressed data hide behind the image file using proposed steganography algorithm. Proposed steganography algorithm is the modified version of standard LSB method. Cover file size of proposed steganography algorithm is same as in standard LSB but the PSNR values get improve in proposed steganography algorithm.

Steps of proposed steganography algorithms are as follows:

1. Take an image cover file as an input having pixels 8/3 times the bit in compressed secret cipher prepared in previous step.

2. Now, hide all the bits of compressed secret cipher behind cover image file using standard LSB method. During this process replace the bits of secret cipher by least significant bit of R, G & B component of image pixel.

3. Next, here some analysis will be performed to increase the PSNR value. All the pixels that hide the secret data divided into four groups on the basis of their 6th & 7th position bits. If both the are 00 then they belong to group 0, if they are 01 then they belong to group 1, if 10 then they belong to group 3 else group 4. Now, check how many pixels have been changed in each group due to hiding secret data. If any group contains more than fifty percent changes then invert all the least significant bit else remain same.

   For example, let consider a string 1011 is a secret binary string that is to be hide and the four pixels are 10101100, 01010101, 11011100 and 00010101. All belongs to group 3, now after hiding string 1011 using LSB method pixels will become 10101101, 01010100, 11011101 and 00010101. So out of 4 pixels of group 3, 3 pixels get changed i.e. more than fifty percent, therefore all the LSB of group 3 will be inverted. So the pixels now become 10101100, 01010101, 11011100 and 00010100. On comparing with the original pixels out of four only one pixel has changed therefore distortion gets reduced compared to original LSB method.

4. Exit

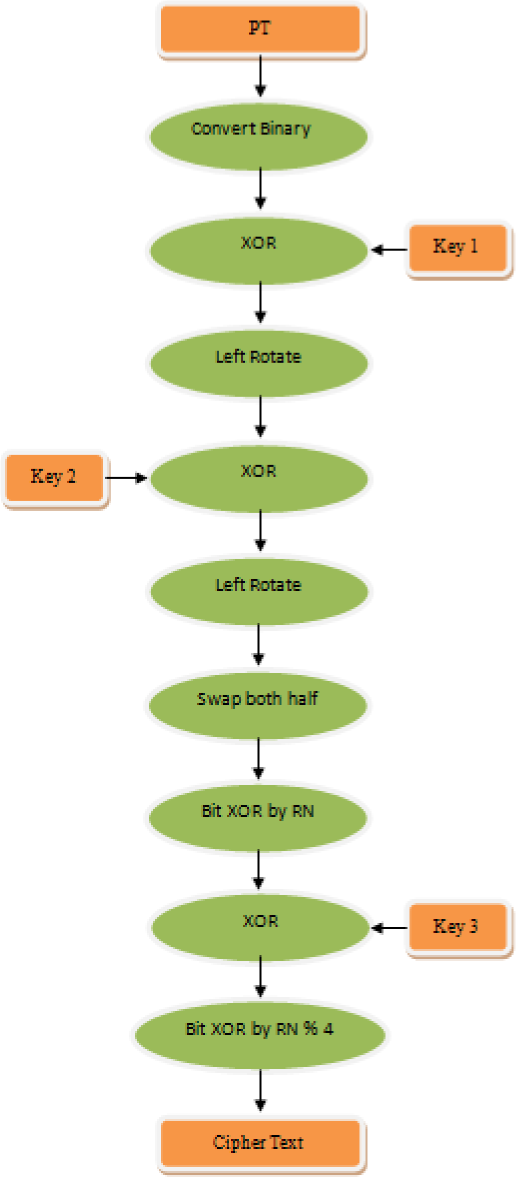

Figure -3: Block diagram of Proposed Encryption Block

4. PERFORMANCE ANALYSIS

In previous sections, authors have discussed various latest researches done in order to improve the quality of security also proposed their own novel algorithm. Also designing of novel algorithm keep no sense, if it is not proper analyzed and compare with the existing algorithm to know whether it good enough to replace them or not. To evaluate the performance of encryption algorithm two main parameters has been considered first: Timing and second is avalanche effect. Also, to evaluate the performance of steganography algorithm PSNR value and cover file size has been considered.

4.1 Analysis encryption and Decryption algorithm

There are many encryption/decryption algorithms that are used to provide confidentiality on the data but there is always a competition to develop an algorithm that is not only secure but also time efficient too. Many researchers have tried to do so, but the problem with their research was on improving the time efficiency, security of the algorithm degrades or if tried to improve security, time efficiency degrade.

4.1.1 Time Analysis: It is necessary for any algorithm that, it should be time efficient. Encryption/Decryption algorithm is used for confidentiality, but this confidentiality is applied many times on real time data. If the encryption/decryption algorithm is not time efficient than it cannot be used for real time transmission. Time Efficiency of encryption/decryption algorithm of all discussed algorithms in section II and proposed algorithm is shown in TABLE 1 & GRAPH 1 shows its graphical representation.

From Graph 1, it is clearly seen that Proposed Algorithm, Paper [1] & BEST encryption time is much lesser than the other existing encryption algorithm. It shows the efficiency of Proposed Algorithm, Paper [1] & BEST. It proves that Proposed Algorithm, Paper [1] & BEST can be suitable real time communication.

4.1.2 Security Analysis: Another important feature to test the encryption/decryption algorithm is its security. An algorithm which is time efficient but not secure is no for use. To test the security of encryption decryption algorithm avalanche effect is calculated.

Table -1: Comparison of Encryption Time

File Size in KB	Algorithm				
	Execution Time in Second				
	Proposed Algorithm	Paper [1]	NJJSAA	DJMNA	BEST
5 KB	0.078	0.150	3.201	16.449	0.127
10 KB	0.405	0.685	6.681	23.523	0.678
20 KB	1.052	1.171	14.038	34.694	2.319

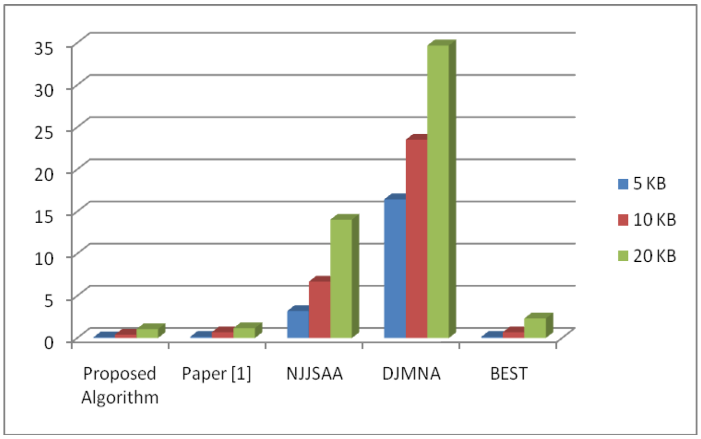

Chart -1: Comparison of Encryption Time

Avalanche effect is one of the parameter used to test the security of any cryptography algorithm. According to avalanche effect an algorithm is consider secure if it generates two cipher text for two different keys (having difference of only one bit) for the same message then the bit difference in both cipher text should be 50%. This is an idle condition; algorithms closed to the idle condition are considered more secure than the other which is far from idle condition. Avalanche effect of the proposed encryption algorithms and its comparison with others is shown in TABLE 2.

Avalanche effect of all the algorithms is approximately same and near to the idle condition except the BEST algorithm as its avalanche effect is very poor. Graph 2 shows the graphical representation of TABLE 2

Table -2: Avalanche Effect

File Size in KB	Proposed Algorithm	Paper [1]	NJJSAA	DJMNA	BEST
	50.12%	49.63%	49.41%	49.01%	9.25%

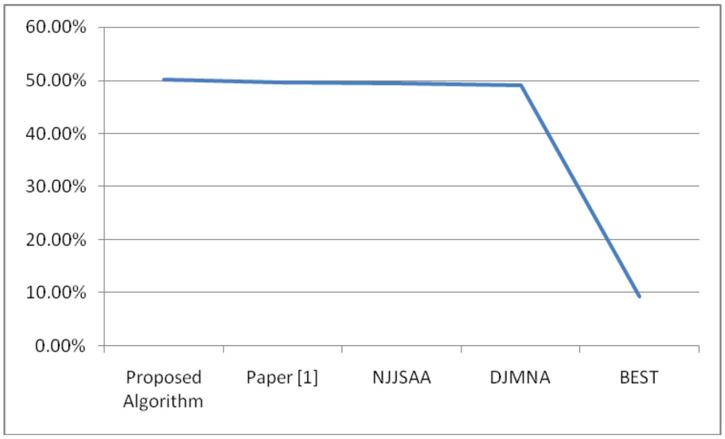

Chart -2: Avalanche Effect

4.2 Performance Analysis of Steganography Algorithm:

Here, analysis of steganography algorithm is done and compare it with others. To evaluate steganography there PSNR value is computed.

4.2.1 PSNR Value: PSNR is peak signal to noise ratio. PSNR is used to check the distortion between stego image and the original Image. If the distortion is less then it will be difficult to guess the presence of secret message behind the cover file but if distortion is more it will be easy to guess the presence of secret information.

If the PSNR value is high it means distortion is less, but if PSNR value is low it means distortion is high.
The comparison of PSNR value of all steganography algorithms discussed in Section II and proposed algorithm is shown in Table 3 and its graphical representation is shown in Graph 3.

From Graph 3, it is clearly seen that PSNR value of Paper [1] is high as compared to other research work.

Table -3: PSNR value comparison of steganography algorithms

File Size in KB	Proposed Algorithm	Paper [1]	Paper [2]	Paper [4]	Paper [5]
PSNR Value	84.11	70.63	56.439	44.465	6.44

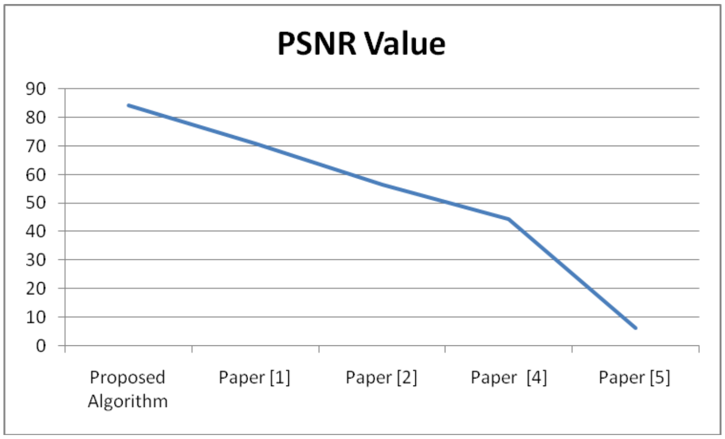

Chart -3: PSNR value comparison of steganography algorithm

5. CONCLUSION

With the rapid development in the field of digital world, it is found that improvement in the existing algorithm is necessary. Many researchers have done their research in this direction but all of them get fail in order to develop completely secure algorithms, some of them have efficiency on some parameters but degrade there quality on other parameters. This paper have proposed their own algorithm in a same way but its implementation results shows that it is efficient compare to all other existing algorithms. Also not only efficient but the proposed algorithm is secure too. Its time efficiency makes it suitable to use in real time communication, it proves itself ideal for ad hoc network not only because of its time efficiency but its simplicity makes it preferable for ad hoc network as it consume less battery.

REFERENCES

[1] Dilpreet Kaur, Harsh Kumar Verma, Ravindra Kumar Singh, " A Hybrid Approach of Image Steganography International Conference on Computing, Communication and Automation (ICCCA2016)", 2016 IEEE

[2] M.K Ramaiya. ; N.Hemrajani, ; , A.K Saxena. "Security improvisation in image steganography using DES" IEEE 3rd International on Advance Computing Conference (IACC), Publication Year: 2013, Page(s): 1094 – 1099.

[3] V. Saravanan, A. Neeraja, "Security Issues in Computer Networks and Stegnography", Proceedings of7'h International Conference on Intelligent Systems and Control (ISCO 2013).

[4] Amitava Nag, Saswati Ghosh, Sushanta Biswas, Debasree Sarkar, Partha Pratim Sarkar "An Image Steganography Technique using X-Box Mapping" IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012

[5] Thomas Leontin Philjon. and Venkateshvara Rao. "Metamorphic Cryptography - A Paradox between Cryptography and Steganography Using Dynamic Encryption" IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011

[6] Debanjan Das, Megholova Mukherjee, Neha Choudhary, Asoke Nath, "An Integrated Symmetric key Cryptography Algorithm using Generalised modified Vernam Cipher method and DJSA method: DJMNA symmetric key algorithm" World Congress on Information and Communication Technologies-2011

[7] Akhil Kaushik, AnantKumar and Manoj Bamela " Block Encryption Standard for Transfer of Data " IEEE International Conference on Networking and Information Technology 2010

[8] Neeraj Khanna, Joyshree Nath, Joel James, Amlan Chakrabarti, Sayantan Chakraborty, Asoke Nat, "New Symmetric key Cryptographic algorithm using combined bit manipulation and MSA encryption algorithm: NJJSAA symmetric key algorithm", IEEE-2011

[9] RigDas and Themrichon Tuithung "A Novel Steganography Method for Image Based on Huffman Encoding" IEEE 2012

[10] R.P Kumar, V. Hemanth, M "Securing Information Using Sterganoraphy" International Conference on Circuits, Power and Computing Technologies (ICCPCT), Publication Year: 2013 , Page(s): 1197 – 1200

[11] G Prabakaran, R. Bhavani, P.S. Rajeswari, "Multi secure and robustness for medical image based steganography scheme" International Conference on Circuits, Power and Computing Technologies (ICCPCT), Publication Year: 2013 , Page(s): 1188 – 1193

[12] Rengarajan Amirtharajan\ Anushiadevi .R2, Meena .y2, Kalpana. y2 and John Bosco Balaguru "Seeable Visual But Not Sure of It" IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012

[13] L.Jani Anbarasi and S.Kannan "Secured Secret Color Image Sharing With Steganography" IEEE 2012

[14] G.Karthigai Seivi, Leon Mariadhasan, K. L. Shunmuganathan "Steganography Using Edge Adaptive Image" IEEE International Conference on Computing, Electronics and Electrical Technologies [ICCEET] 2012

[15] AmrM. Riad, Amr H. Hussein and AtefAbou EI-Azm "A New Selective Image Encryption Approach using Hybrid Chaos and Block Cipher "The 8th International Conference on INFOrmatics and Systems (INFOS2012) - 14-16 May Computational Intelligence and Multimedia Computing Track

[16] Arun Raj R, Sudhish N George and Depths P. P. "An Expeditious Chaos Based Digital Image Encryption Algorithm" 1st Int'l Conf. on Recent Advances in Information Technology | RAIT-2012

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

[18] Somdip Dey, Kalyan Mondal, Joyshree Nath, Asoke Nath "Advanced Steganography Algorithm Using Randomized Intermediate QR Host Embedded With Any Encrypted Secret Message: ASA_QR Algorithm" I.J.Modern Education and Computer Science, 2012, 6, 59-67

[19] S.Premkumar, A.E.Narayanan "Steganography Scheme Using More Surrounding Pixels combined with Visual Cryptography for Secure Application "International Conference on Computing and Control Engineering (ICCCE 2012), 12 & 13 April, 2012

[20] Abhishek Gupta, Sandeep Mahapatra and, Karanveer Singh " Data Hiding in Color Image Using Cryptography with Help of ASK Algorithm" 2011 IEEE

[21] Ashwak M. AL-Abiachi, Faudziah Ahmad and Ku Ruhana "A Competitive Study of Cryptography Techniques over Block Cipher" UKSim 13th IEEE International Conference on Modelling and Simulation 2011

[22] Guy-Armand Yandji, Lui Lian Hao, Amir-Eddine Youssouf and Jules Ehoussou RESEARCH ON A NORMAL FILE ENCRYPTION AND DECRYPTION" IEEE 2011

[23] Dripto Chatterjee, Joyshree Nath, Suvadeep Dasgupta, Asoke Nath "A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm" published in 2011 International Conference on Communication Systems

and Network Technologies, 978-0-7695-4437-3/11 $26.00 © 2011 IEEE

[24] Rosziati Ibrahim and Teoh Suk Kuan "Steganography Algorithm to Hide Secret Message inside an Image" Computer Technology and Application 2 (2011) 102-108

[25] Danah Boyd and Alice Marwick "Social Steganography: Privacy in Networked Publics" ICA 2011

[26] Ashwak M. AL-Abiachi, Faudziah Ahmad, Ku Ruhana " A Competitive Study of Cryptography Techniques over Block Cipher" 13th IEEE International Conference on Modelling and Simulation 2011 UKSim