A Vision on Text Steganography with proper Investigation Report to Identify the Associated Problem

Rajeev Gupta[#], Dr. Vivek Sharma[*]

[#]Master of Technology, (Computer Tech. & Application)
TIT Advance, Bhopal, INDIA

Abstract*—Security is one of the major issues now days. As we are moving towards modern technologies, risk on our confidential information also increases rapidly. Today's, all of us are very much dependent on digital world. Communications, Entertainment, Data Storage, Business and Banking all are part of our daily life in digital world. To aim at all, there is a need to upgrade or construct new security algorithms or design such that it should be efficient to cope up with latest modern technologies and parallel enough secure against latest attack. Many researchers have done their research in the same field and presents there solutions that can give better results of the above discussed problem. There are many type of security; this paper strictly focused on confidentiality and discussed all those solutions after doing deep inspection on it.*

Keywords - *Computer Security, Steganography, MSA Algorithm, Encryption Decryption Algorithm*

I. Introduction

Securing information in digital world is vital today. There are many people who continuously try to steal this information for their own benefits. There are many different algorithms exist that provides the security in efficient way. Security implies confidentiality, integrity and authenticity. All together provides the complete security. Confidentiality in digital word means ensuring that the secret information will be read or understand by authenticated persons only. If somehow, an unauthorized person will gain the information then also they will not be able to read it. Integrity ensure that receiver receive the same copy that sender send, no one during transmission change the content, if someone succeed to do that then it must be identified at receiver end. Authentication ensures that communication or transfer of file must be done between authorized person and no one deny after transmission or receiving the file. This paper purely bound itself on confidentiality. Confidentiality can be achieved by two ways: either by using any encryption/ decryption algorithm or by using any steganography algorithm. Sometimes both the algorithm gets fused to get better results. Encryption is an art of shuffling the arrangement of characters or replacement of characters of secret information such that no one can understand its real meaning. This shuffling is done by using key, so that in can be arrange again by the person authorized to do that. The shuffle data is also called cipher data. AES and DES are some standard encryption algorithms approved by government of many countries.

DES algorithm first published in 1975 and AES algorithm published in 1998 but today we work on micro devices where these algorithms are not as feasible as it should be.

On the other end, Steganography is different type of algorithm used to ensure confidentiality. Steganography hides the information behind any media file (Text, Image or Audio/Video)in such a way that no one can guess the presence of hidden secrecy. LSB (Least Significant Bit) method is the most popular steganography method. In this, information is first converted into binary format and then each bit of secret information is replaced with the least significant bit of media file that use as a cover file.

II. LITERATURE SURVEY

In order to improve the security, encryption/decryption algorithm combined with steganography algorithm. There are already many algorithms exist that proves themselves as a standard. But today's almost all those algorithms seems in efficient according to the needs that is required now days. Many researchers have done their research in this direction and proposed theirown models that fulfil this gap. This paper discusses many such algorithms that work on text steganography and presented their comparative analysis to understand them deeply and to find the better one.

In 2012 [3], a novel approach was designed on text steganography, where the researchers have presented a complete new approach towards hiding text behind any text file. In this research, researchers first encrypt the secret information by using their proposed (called

MGVCM) encryption algorithm and then hide the cipher behind any text cover file. The concept used to hide the text behind any text is based on ASCII values of characters. In English ASCII value of space is 32 and a character called invisible character look like a space having ASCII value 160. So there are two different characters which look similar but having different ASCII value. Therefore to hide secret information, it is first converted into binary format and then hides each bit behind text spaces of cover file by using following rule.

Rule: if secret information bit is 0 then blank spaces remain same and if secret information bit is 1 then replace the blank space by character having ASCII value 160.

By doing this, cover file look same as it looks previous and cannot be easily detect by necked eyes.

The major problem identified by this paper in the above algorithm is the size of cover file. Generally, a character is represented by 8 bits, so to hide a single character there is a need of 8 blank spaces therefore to hide a sentences or a paragraph having α characters, need a cover file must have blank spaces equal to 8* α. This makes the cover file size very large, hence time required to transmit this file is high which seems like a huge drawback of this research.

Next, in 2013 [2], a new concept was introduced which is based LSB method discussed in SECTION I. This research proposed a method in which the secret information is first converted into hexa-decimal format. Here, cover file should be any MS word file, where text can be written in black colour generally.It is pre-decided that which hexadecimal character will get which colour code. (All the colour codes are different shades of black which cannot be detecting by necked eyes). Now, every hexadecimal character of secret information hides behind cover text file by doing re-colouring of cover file characters according to hexadecimal codes. For example if we have character ‘e’ in cover file and we have to hide hexadecimal ‘8’ behind it and the colour code decided for ‘8’ is (0,2,2) (i.e. RGB values), then character ‘e’ will be coloured by (0,2,2).

Here, the size of cover file is low, but it seems like its distortion in cover file should be high as compared to standard LSB method. (Parameter analysis of theses algorithms is discussed in SECTION III).

Latest, in 2004 [1] Researchers have proposed there new algorithm which is again a fusion of encryption/ decryption and steganography algorithm. Here, secret information if first encrypted using DES encryption algorithm and then hides behind a text cover file. The hiding process takes a text cover file which is actually a linear array of English characters and digits. Next it counts the frequency of characters in cipher text with its respective positions. Next retrieve the position of encrypted character in cipher text and compare it with the character in cover file and calculate the position of that character in cover file. Treating the position as ASCII value and the character represent by this ASCII value replaced the encrypted character.

Next this algorithm also generates the puzzle, which is divided into two sections. First section holds the cipher character and second section hold the position of character. Also in second section, the position is represented by using some arithmetic operations.

The problem identified with this paper is in its steganography process, which completely change the shape of cover file, which means huge distortion and easy to guess the presence of secrecy. Also the concept of embedding puzzle seems negative as it increases cover file size and make nothing difficult for intruder to decrypt the cipher.

This section just discusses the latest research done on text steganography and the problem identified at first glance. In the next section, paper discusses the comparative analysis of the implementation results of all this researches.

III IMPLEMENTATION ANALYSIS

This section gives a comparative analysis of all the algorithms discusses in SECTION II to deeply investigate the efficiency and security of existing algorithms.

To judge all the algorithms equally, all the algorithms were implemented and tested on single system so that all the conditions for all the algorithms are same. The presented results are performed on a system having following configuration:

Intel Core I5, 2.40 Ghz Processor, 4 GB of RAM and 64 Bit, Window 7 Home BasicOperating System.

A. Analysis of encryption/decryption algorithm:

There are many encryption/ decryption algorithm exist but not all are the best in all respective. To know the best algorithm it should be tested under some parameters. To test the performance of any encryption/ decryption algorithm execution time efficiency and security (which can be calculated using avalanche effect) analysis is must.

- *Analysis of execution time:*

Execution time is the total time required to convert the secret information into cipher text. Table 1 shows the execution time of encryption algorithm RJDA [3] &DES [1].

TABLE 1
EXECUTION TIME ANALYSIS OF RJDA [3] & DES [1]

File Size (in KB)	Execution Time (in Seconds)	
	RJDA [3]	DES [1]
1 KB	9.364	0.084
5 KB	17.241	0.274
10 KB	25.364	0.721

Now, from Table 1 it is clear that the encryption algorithm use in RJDA [3], is not time efficient as compared to DES algorithm. It means for a large file, it takes a huge time to encrypt hence cannot be use for large files. Also, it cannot be used in real time communication because of its in efficiency in timing. Ad-Hoc or micro devices always preferred light weighted algorithms which are fast and efficient hence RJDA is also least preferable in these.

For better understanding of Table 1, in terms of how these algorithm progress when file size increase, Graph is plotted. Graph of Table 1 is shown in Fig 1.

- *Analysis of Avalanche effect:*

Analysis of execution time to calculate the performance of encryption/decryption algorithm is not enough. It is must to do an analysis on its security. For security analysis, avalanche effect is calculated which state that if the internal structure of encryption algorithm is enough robust than it should generate 50% bit difference in cipher while changing a single bit in key for the same text. This is an idle condition, an algorithm close enough to this condition is consider more secure.

Avalanche effect of RJDA [3] & DES [1] is shown in Table 2 and its graphical representation shown in Fig 2.

Now, from the above table it is clear that both the algorithms are closed to avalanche effect and equally secure. Hence both the algorithms can be used in a noisy channel.

B. *Analysis of Steganography algorithm:*

Here, this paper analysis the text steganography algorithms proposed in paper [1], paper [2] and paper [3]. Again to evaluate the performance of steganography two parameters are used. First PSNR value and second is size of cover file.

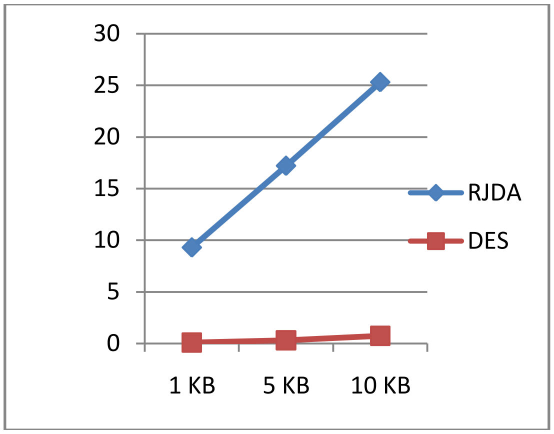

Fig 1: Execution Time Analysis of RJDA [3] & DES [1]

TABLE 2
AVALANCHE EFFECT OF RJDA [3] & DES [1]

Key	RJDA [3]	DES [1]
Key-1	48.62%	49.41%
Key-2		

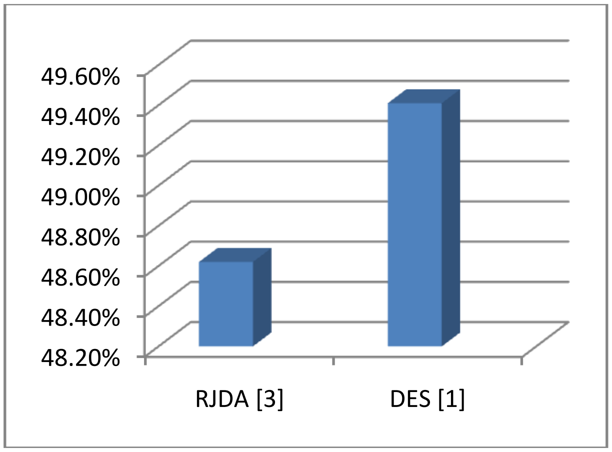

Fig 2 Avalanche Effects of RJDA [3] & DES [1]

- *Analysis of cover file:*

It is important to keep the size of cover file low, because if the size of cover file is large then the time required transmit or space required to store it must be more.

Cover file required to hide the information in RJDA is much more than the other as it needs eight spaces to hide each character which make the cover file size very high. On the other end paper [2] require less cover file as compared to standard LSB method or RJDA algorithm. As it requires cover file should have atleast four times more character than the secret information character. Where as the file size of cover file in paper [1] is constant. So on the basis of cover file size it can be concluded that algorithm proposed in paper [1] is best.

Analysis of PSNR value:

PSNR value is peak signal to noice ratio which is used to calculate the distortion in cover file after embedding the secret information. It is simply nderstood that more distortion in cover file make easy to intruder to guess the presence of secrecy.

Higher the PSNR value means lower the distortion. PSNR value of all the three papers and standard LSB algorithm are shown in TABLE 3 and Graph 3 shows its graphical representation.

TABLE 3:
PSNR VALUE COMPARISON OF PAPER [1], PAPER [2], PAPER [3] AND STANDARD LSB

	Paper [1]	Paper[2]	Paper [3]	Standard LSB
PSNR Value	9.25%	62.46%	19.13%	62.94%

Hence, it is clear from Table 3 that algorithm presents in paper [1] is worst as it can be easily guessable and still standard LSB having less distortion.

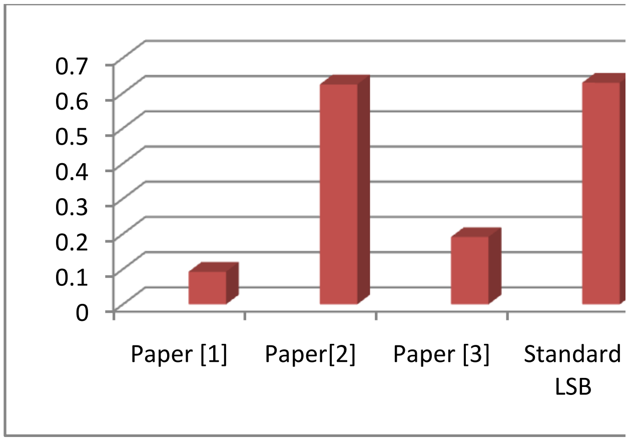

Fig 3: PSNR value comparison of paper [1], paper [2], paper [3] and standard LSB

IV. CONCLUSION

After detail study of all on text steganography and encryption/ decryption algorithm, it is found that all the existing algorithms are not enough secure in all prospective. Each algorithm has their merits and demerits. But as discussed, security in digital world cannot be compromised. In order to meet the requirement there is a need to design an algorithm that set the standard algorithm as a base and then improves some result without affecting the others.

REFERENCES

[1] Md. Palash Uddin, Mousumi Saha, Syeda Jannatul Ferdousi, Masud Ibn Afjal, Md. Abu Marjan, "Developing an Efficient Solution to Information Hiding through Text Steganography along with Cryptography" The 9th International Forum on Strategic Technology (IFOST), October 21-23, 2014, Cox's Bazar, Bangladesh, IEEE

[2] Xing Tang, Mingsong Chen, "Design And Implementation Of Information Hiding System Based On RGB", 2013 IEEE.

[3] Rishav Ray, Jeeyan Sanyal, Debanjan Das, Asoke Nath. "A new Challenge of hiding any encrypted secret message inside any Text/ASCII file or in MS word file: RJDA Algorithm". 2012 IEEE International Conference on Communication Systems and Network Technologies.

[4] C. K Mulunda, P. W .Wagacha and A. O. Adede, Genetic Algorithm Based Model in Text Steganography, The African Journal of Information Systems, Vol. 2 Issue 5, pp. 131-144, October 2013.

[5] An Integrated Symmetric key Cryptography Algorithm using Generalised modified Vernam Cipher method and DJSA method: DJMNA symmetric key algorithm : Debanjan Das, Joyshree Nath, Megholova Mukherjee, Neha Choudhary, Asoke Nath: Communicated for publication in IEEE International conference WICT 2011 to be held at Mumbai Dec 11-14, 2011.

[6] 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.

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

[8] 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

[9] 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

[10] 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

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

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

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

[14] 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

[15] 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

[16] Rengarajan Amirtharajan, Anushiadevi, Meena, Kalpana 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

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

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

[19] 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

[20] 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

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

[22] 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

[23] 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

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

[25] 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

[26] Anderson, R. J., and F.A.P. Petitcolas. 1998. "On The Limits of Steganography". IEEE Journal of Selected Areas in Communications. 16(4): 474-481.

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

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

[29] William stallings, "Cryptography and Network Security:Principles & Practices", second edition.
http://en.wikipedia.org/wiki/Peak_signal-to-noise_