IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 3, Ver. VII (May-Jun. 2014), PP 106-110
www.iosrjournals.org

Comparative analysis of Stegnography Algorithms on the Basis of PSNR value & cover file size

Shubhi Jain[1], Sini Shibu[2]
[1]*M.Tech. Scholar, Dept. Of Computer Science Engineering, NIIST Bhopal (M.P.)*
[2]*Assistant Prof. Dept. Of Computer Science Engineering, NIIST Bhopal (M.P.)*

Abstract: *With the rapid growth in the field of technology, there is always a requirement of development of fast and secure algorithms. Steganography is used to provide confidentiality over the transmitted data or the stored data. There were many steganography algorithms proposed to provide security but there is always a competition to develop a algorithm which is fast, secure, having high PSNR value and less cover file size. In this paper, authors have discussed such papers and compare it with each others.*

Keywords: *Computer Security, Network, Encryption, Decryption, Algorithm, Cryptography, Symmetric Key*

I. Introduction

The rapid growth in the demand and consumption of the digital multimedia content in the past decade has led to some valid concerns over issues such as content security, authenticity, and digital rights management. Multimedia data hiding, defined as imperceptible embedding of information into a multimedia host, provides potential solutions, but with many technological challenges.

The first problem that usually occurs is that of embedding high volume of information in an image without incurring any perceptual distortion, and achieves robustness against compression and attacks. Data hiding can be defined more formally as the process by which a message signals or signature is imperceptibly embedded into a host or cover to get a composite signal.

Various digital data hiding methods have been developed for multimedia services, where a significant amount of secret data is embedded in the host signal. The hidden data should be recoverable. It should also be retrieved only by those authorized. The main problem of file hiding in another host image or other files is a large amount of data that requires a special data embedding method with high capacity as well as transparency and robustness.

A possible formula of the process can be given as:
Cover image + Message to covert + Stego-key (the password) = Stego image

A Steganography system is usually composed of insertion and extraction subsystems. The insertion system takes a host file, a prepared message file or the data which is to be furtive from the view, and a key to insert the message into the host for creating a cover host. This is referred to as the embedding process. The coverhost is then stored or transmitted. The extraction system operates in reverse. It takes a covert host and a key as input and extracts the message. The modern Steganography techniques are such efficient that data can be transmitted effortlessly over internet devoid of anyone knowing the existence.

There is always a competition to develop steganography algorithms which provide high security, also with security researchers try to gain this security with keeping low cover file size and high PSNR value.

In this paper, authors have discussed different steganographic algorithms, implement it and compare it with each other.

II. Literature Survey

In this section, authors have discussed the various researches done on steganography algorithm. As discussed by Manoj Kumar Ramaiya, Naveen Hemrajani, Anil Kishore Saxena [1], presents its unique technique for image staganography based on Data Encryption Standard using the strength of S Box mapping. In this paper[1], authors have modified the DES algorithms and use this algorithms to encrypt the secret image pixel before hiding it behind the cover image file. After encrypting the entire pixel, convert it into bit stream. This bit stream is hiding behind the pixel of cover image. Every two least significant bit of cover image replaced with the two bits of a bit stream till all the bits are completed. In this technique, image is first encrypted by modified DES algorithm so that if someone gain to detect presence secret image, still it is not possible to gain the original secret image without knowing the key. Again, this technique hides bits of secret image behind two least significant bit of cover image. Hence size of cover image should be at least twice in width and height. But changing only in least two significant does not affect the quality of cover image. It is nearly impossible to detect the difference between original image and stego image with necked eyes.

Thomas Leontin Philjon. J, Venkateshvara Rao. N [2] presents a new technique in its paper. This technique first encrypts the message with image and generates a cipher image now; this cipher image is manipulated with the cover image and generates an intermediate text. This intermediate text is again encrypted with the same encryption algorithm and generates a cipher image. Now, this algorithm gains the security by encrypting the secret message twice. Also the size of cover image should be at least equal to size of cipher image. The main problem with this technique is that it can easily detectable by necked eyes that something is hidden in cover image because direct manipulation with the cover image degrades the quality of stego image.

III. PERFORMANCE ANALYSIS

This section is providing analysis of the above discussed algorithms on the basis of different parameters like Security, Cover file size, Timing and PSNR value. Dot Net implementation has used to test these algorithms. For experiment, Intel Core i5 2.40 Ghz, 4 GB of RAM and Window-7 Home Basic SP1, have used in which performance data is collected.

Time Analysis: The main parameter to analysis any algorithm is its speed. Any algorithm is judged on the basis of its speed. An algorithm which takes less time is considered better than other which takes more time.

Timing is also very important because the algorithm which takes less time is considered to be suitable for Ad-Hoc network because it consume less battery than other. Also time efficient algorithms are suitable for real time transmission.

Table 1: Encryption Timing Analysis between Paper [1] and Paper [2].

File Size in KB	**Algorithm**	
	Execution Time in Second	
	Paper [1]	Paper [2]
1 KB	0.027	0.075
6 KB	1.575	2.172

Here, Table 1 shows the Encryption timing analysis between paper [1] and paper [2]. It is cleary seen from the table that technique used in paper[1] is faster than paper[2]. Graphical representation of Table1 is shown in Figure1.

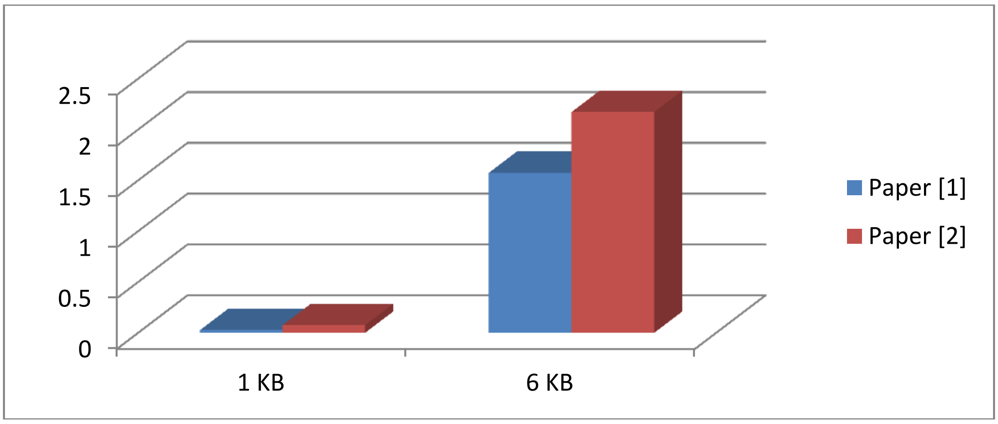

Figure1: Encryption Timing analysis between Paper[1] and Paper [2].

Figure 1 shows the timing analysis between Paper [1] and Paper [2]. Blue block represents the Paper [1] and Paper[2] is represented by red block.

Hence it can be concluded that Paper[1] is time efficient than Paper[2].

Table 2 shows the decryption time analysis between paper[1] and paper[2] and Figure 2 shows its graphical representation. It is clearly viewed from the graphical representation that Paper[2] takes almost the same time to extract the secret data from the cover file whereas Paper[1] takes much more time than the encryption time to extract the secret file from the cover file. Hence decryption of Paper [1] is not time efficent.

Table 2: Decryption Timing Analysis between Paper [1] and Paper [2].

File Size in KB	**Algorithm**	
	Execution Time in Second	
	Paper [1]	Paper [2]
1 KB	0.031	54.087
6 KB	1.582	2.175

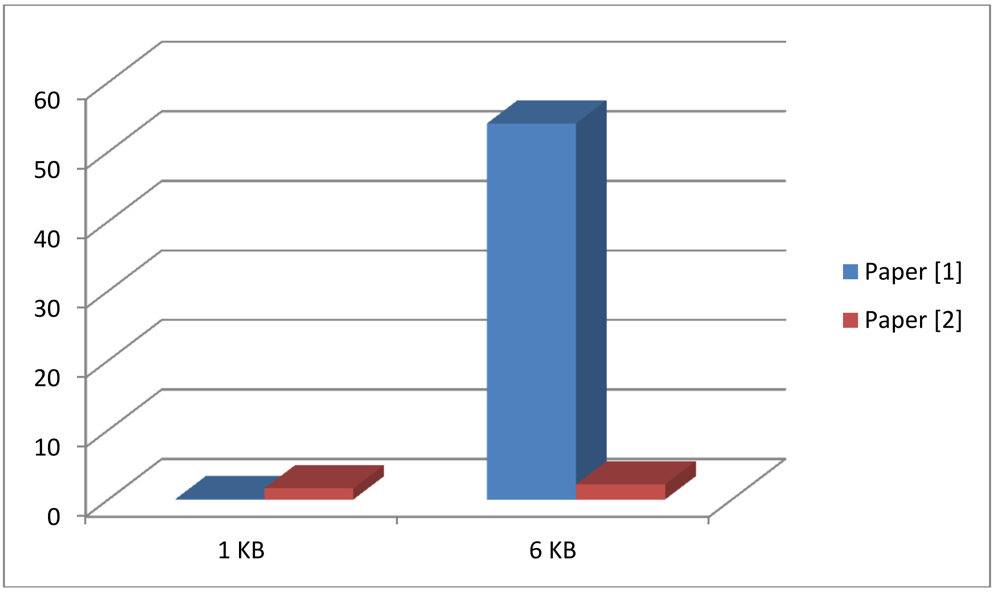

Figure2: Decryption Timing analysis between Paper[1] and Paper [2].

IV. PSNR Value Analysis

PSNR is the peak signal to noise ratio. It is used to calculate the deviation of stego image with the original image. If the PSNR value of an algorithm is high, it means deviation of stego image with respect to original image is less. If the deviation of the stego-image with the original image is less it means it is hard to detect the presence of secret hiding but if deviation is more it mean easy to detect the presence of secret hiding.

Authors have compared the PSNR values of both the papers and represented in Table 3.

Table 3: Comparison of PSNR values between Paper [1] and Paper [2]

	Algorithm	
PSNR Value	Paper [1]	Paper [2]
	44.32	6.42

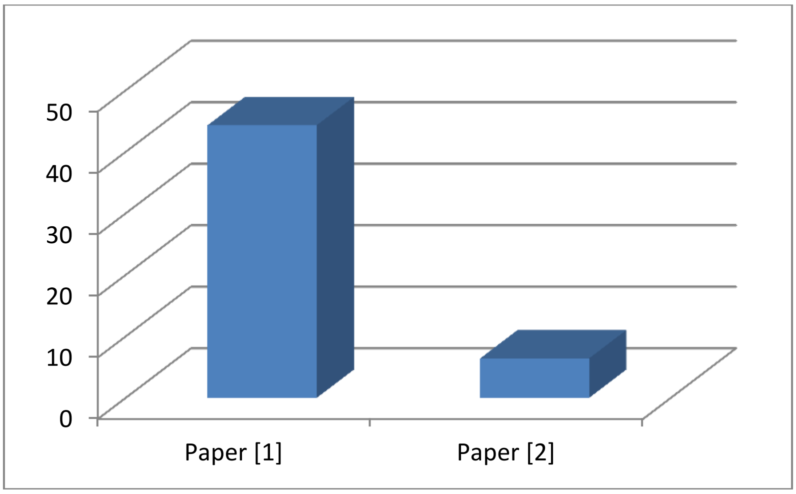

Figure3: Comparison of PSNR values between Paper [1] and Paper[2]

A graphical representation shown in figure 3 clearly shows that PSNR value of Paper [1] is much higher than PSNR value of Paper [2]. It means it is hard to detect the presence of hidden text in Paper [1] technique than the Paper [2] technique.

V. Cover file Size Analysis

It is very important to keep the size of cover file less in any stego image. As the size of cover image increases transmission time also increases therefore for keeping algorithm for fast communication it is essential to keep the size of cover file not very large.

In Paper [1], it is required that size of cover image must be at least twice of secret image in length and width both.

In Paper [2], the size of cover image must be at least equal to the size of cipher image. It means this technique requires less cover file size as compared to cover file size in Paper [1].

Security: In terms of security, both the algorithms are enough secure. Paper [1] uses modified DES encryption before hiding the secret file whose internal structure is enough secure but the problem is in its key which is only 16 bits long. So it requires only 216 combinations which are possible to calculate in reasonable time. Also hiding of secret file starts from the first pixel to all the next pixels so if someone gets the hint of hidden file it can easily extract from the cover file size.

Paper [2] is more secure than Paper [1] because of using encryption algorithm twice also it is not easy to extract the hidden file from the cover file because of its manipulations with pixel of cover file with cipher file.

VI. Conclusion

This paper presents the complete discussion between two different type of steganography algorithm. It is concluded that to prepare efficient steganography algorithm, It is necessary that it should be time efficient, should use less cover file size, having high PSNR value and also should be enough secure so that no one gain the access over the confidential data. Many researchers have tried to work on this but cover file size and PSNR value are directly proportional to each other, if PSNR value increases cover size also increases and if cover size reduces PSNR value also reduces.

Future Work

This paper shows that there is requirement to develop such a secure steganography algorithm having high PSNR value with less cover file size.

REFERENCES

[1] Manoj Kumar Ramaiya, Naveen Hemrajani, Anil Kishore Saxena, “Security Improvisation in Image Steganography using DES”, IEEE-2012.

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

[3] Yambin Jina Chanu , Themrichon Tuithung , Kh Manglem singh,“ A Short Survey on Image Steganography and Steganalysis Technique “ , IEEE Trans, 2012 science and Management (ICAESM- 2012) 709 -713.

[4] W. Luo, F. Huang, J. Huang, Edge adaptive image steganography based on LSB matching revisited, IEEE Trans. Inf. Forens. Security 5 (2) (2010) 201-214.

[5] Ge Huayong, Huang Mingsheng, Wang Qian , "Steganography and Steganalysis Based on Digital Image", IEEE Trans. International Congress on Image and Signal Processing,(2011) 252-255.

[6] Amitava Nag, Saswati Ghosh, Sushanta Biswas, Debasree Sarkar, Parta Pratim Sarkar " An Image Steganography Technique using X-Box Mapping", IEEE Trans. International Conference Advances in Engineering,

[7] Guilliang Zhu, Weiping Wang, "Digital Image Encryption algorithm based on pixel", ICIS – 2010 IEEE International Conference 29-31 Oct 2010, pp – 769 – 772.

[8] Jasmin Cosic , Miroslav Bacai, " Steganography and Steganalysis Does Local web Site contain "Stego" Contain " , 52 th IEEE Trans. International Symposium ELMAR-2010, Zadar, Croatia 2009 ,pp 85 –88.

[9] Zhang Yun-peng , Liu Wei " Digital Image Encryption Algorithm Based on chaos and improved DES ", System, man and Cybernatics ,SMC 2009 , IEEE International Conference 11-14 Oct 2009, pp 474-479.

[10] Saeed R. Khosravirad, Taraneh Eghlidos and Sharokh Ghaemmaghami, "Higher Order Statistical of Random LSB Steganography", IEEE Trans. 2009, pp 629 - 632.

[11] J. Mielikainen, LSB Matching Revisited, IEEE Signal Process. Lett. 13 (5) (2006) 285-287.

[12] N Provos and P. Honeyman, "Hide and seek: An Introduction to Steganography", IEEE Security and Privacy, 2003, pp32-44.

[13] Donovan Artz" Digital Steganography: Hiding Data within Data ", Los Alamos National Laboratory, IEEE Trans. 2001, pp 75-80.

[14] K Suresh Babu , K B Raja, Kiran Kumar k, Manjula Devi T H, Venugopal K R, L M Pathnaik" Authentication of Secrete Information in Image Steganography", IEEE Trans. 13.

[15] Moerland, T, "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science, www.liacs.nl/home/ trnoerl/privtech.pdf.

[16] Schaefer " A Simplified Data Encryption Standard Algorithm", Cryptologia, January 1996

[17] Data Encryption Standard : http://csrc.nist.gov/publications/fips /fips 46-3 /fips- 46-3.pdf

[18] Advanced Encryption Standard http://csrc.nist.gov/publications/ fips/fips197/fips- 197.pdf

[19] Cryptography and network Security Principles and Practices, Charles Fleeger

[20] William Stallings, "Network Security Essentials (Applications and Standards)", Pearson Education, 2004.