International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 02, February-2015

An Infallible Method to Transfer Confidential Data using Delta Steganography

Anooplal K. S[1].
Student-M.Tech in CSE
Sahyadri College of Engineering & Management
Mangalore, India

Girish. S[2].
Assistant. Professor / CSE
Sahyadri College of Engineering & Management
Mangalore, India

***Abstract*—These days, computers and smart phones are the major mode of communication, which helps us to connect different parts of the world instantly, but safety and security may get compromised. This creates rigorous issues while transferring confidential data. By making use of Steganographic techniques these security threats can be tackled to some extent. In this paper, delta steganographyis proposed, which is a combined form of steganography and delta compression algorithm. Steganography efficiently hide text file inside an image, delta compression comparing stego image and reference image then produce a set of instructions named as delta file. Storing or transmitting a delta file rather than the image can offer significant efficiency gain as well as high security to the confidential data.**

Keywords— Steganography; encryption; delta compression; embedding; extraction.

I. INTRODUCTION

The ancient Greek words "Steganos" and "Graphein" plays a major role in the evolution of the word Steganography, which is presently used in the field of secret communication. Steganography is the practice of hiding secret data inside other media in an effort to keep third parties from knowing that the intended message is even there[3][4][8].

The primary objective of steganography is to avoid drawing attention to the transmission of hidden information. If suspicion is raced, then objective that has been planned to achieve the security of the secret message because if the hackers noted any change in the sent message then this intruder will try to know the hidden information inside the message[1][2].

In steganography, before the hiding process, the sender must select appropriate carrier message, an image. Then select the secret message to be hidden as well as a secret key as pass phrase. A robust steganographic algorithm should be selected which can be able to encrypt the secret message more efficiently.

The sender then sends the hidden message to the receiver by using any of the modern communication technologies. The recipient after receiving the message, decrypt the hidden message using extraction algorithm with secret key[2][6].

In this work, a secure algorithm to hide data inside an image using steganographic technique and a delta compression method is also been implemented to achieve high security and reduced file size.

The paper is organized as follows: Section 2 and 3 describe about steganography and delta compression. Section 4 would be presenting the proposed algorithm. The implementation section is discussed in section 5. Discussion of various results obtained from the testing of the system with various sizes of data is explained in section 6 and finally the conclusion of the paper along with future scope and references.

II. STEGANOGRAPHY

Steganography can be worn to hide secret message intended for a specific individual or group. In this case the aim is to prevent the message being detected by the intruder. Steganography is also widely used in copyright marking, here the message to be inserted is used to assert copyright over a document. In order to ensure data security Steganography and encryption are widely used. However the main difference between them is that with encryption anybody can see that both parties are communicating in secret. Steganography is used to hide the message as well as its existence, thereby ensures complete secrecy. This makes steganography suitable for some tasks for which encryption aren't, such as copyright marking. Adding encrypted copyright information to a file could be easy to remove but embedding it within the contents of the file itself can prevent it being easily identified and removed.

In digital world, both Steganography and Cryptography are used to secure confidential information while communicating. In order to provide better security for the message, both these techniques can be combined. As a result it offers multiple layers of security.

General stenographic approach is shown in figure 1. The cover message is the carrier of the message such as image. The secret message is the information which is needed to be hidden in the suitable digital media. The stego image is the resultant image which we obtained after performing stenographic process that is hiding the secret data in suitable media. The secret key is used to embed the message depending on the hiding algorithms. The embedding algorithm is the way or idea that usually used to embed the secret information in the cover message [5][9].

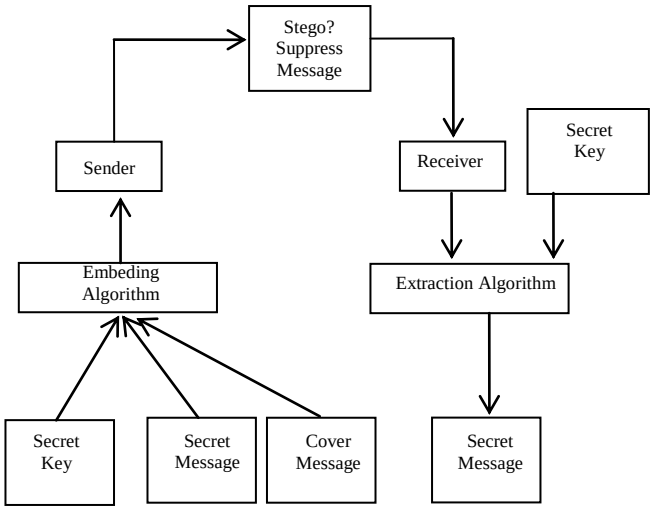


Fig. 1. General Steganography approach.

III. DELTA COMPRESSION

In order to reduce the space consumption and to increase the efficiency of data transfers, delta compression techniques are widely used in the computer networks and in the data storage systems. These delta compression techniques make use of compression which accepts reference source file and the target files as its two inputs. The notations F' denotes secret file, F is reference file and ΔF is delta file. The delta creator locates and copies the difference between the target and source file, comparing only these differences as a delta shown figure 2.

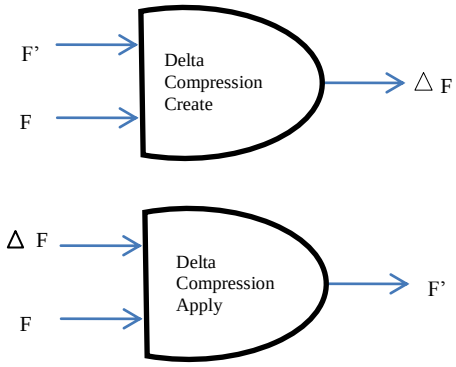


Fig. 2. Delta Compression.

Size (ΔF-F') << Size (F')

IV. PROPOSED ALGOTITHM

In this method, instead of the earlier LSB technique, a more secure approach is used for hiding the data in an image. The hiding process is performed as shown below. Convert cover image into RGB image.

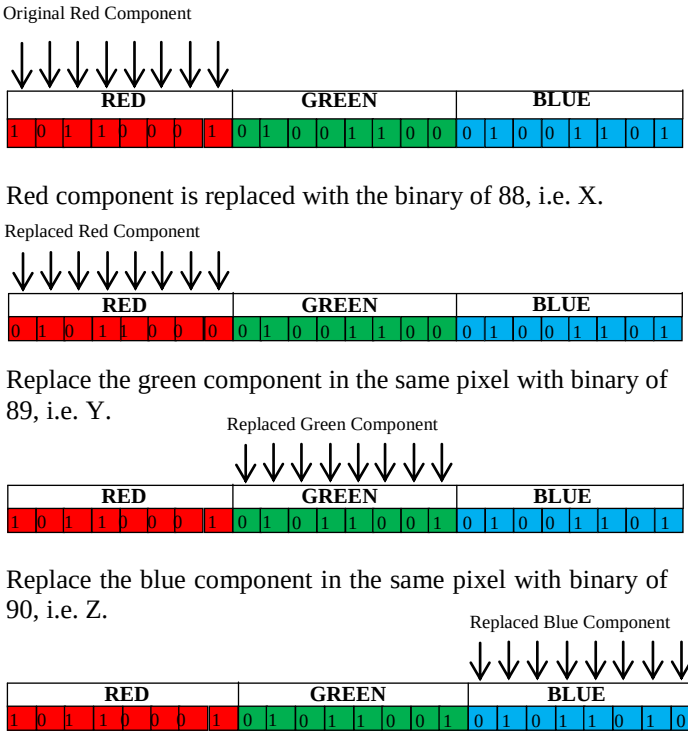
Let the data to be hidden is word "XYZ"

ASCII code of X=88 and corresponding binary is 01011000.

ASCII code of Y=89 and corresponding binary is 01011001.

ASCII code of Z=90 and corresponding binary is 01011010.

Let the RGB component of the first pixel is:-



And process continues.

The resulting stego image that obtained after the algorithm completes its execution is distorted and is easy to detect. So, this is the first level of security, to enhance the security of the secret message we would be use delta compression algorithm here. That compare the RGB value difference between stego image and reference image into a text file named as delta file, this is the second level of security. By looking at the resulting delta file no one would be able to predict that the contents inside the delta file.

The proposed steganographic algorithm comprises of two embedding techniques they are data hiding technique and data extraction technique shown in figure 3. Data hiding technique as the name suggests is used to hide secret message in the cover image, while data extraction technique is used to retrieve the secret message from the reference image with delta file so the confidential data is secured from unauthorized access.

The proposed embedding technique.

Inputs:-Secret text, secret key, cover image.

Output:-Delta file.

Begin

1. Select the Secret Text, call ASCII code generation function.
2. Select an image, Find number of pixels, Convert its RGB components, and calculate number of bits in text file.
3. If calculated bits is less than or equal to number of RGB components, then

Start iteration

Displace red component of first pixel with ASCII value of first character.

Displace green component of first pixel with second character.

Displace blue component of first pixel with third character and store RGB component values.

Select next pixel and reiteration until character get empty.
End iteration
4. Accept secret key and call encryption.
5. Call delta creator and save delta file.

Else
Error, image is of low resolution.
End

Proposed extraction technique.
Inputs:-Reference image, Secret key, Delta file.
Output:-Secret text.
Begin
1. Select delta file.
2. Provide secret key and reference image, and then call extraction function.
3. Display secret message.

End

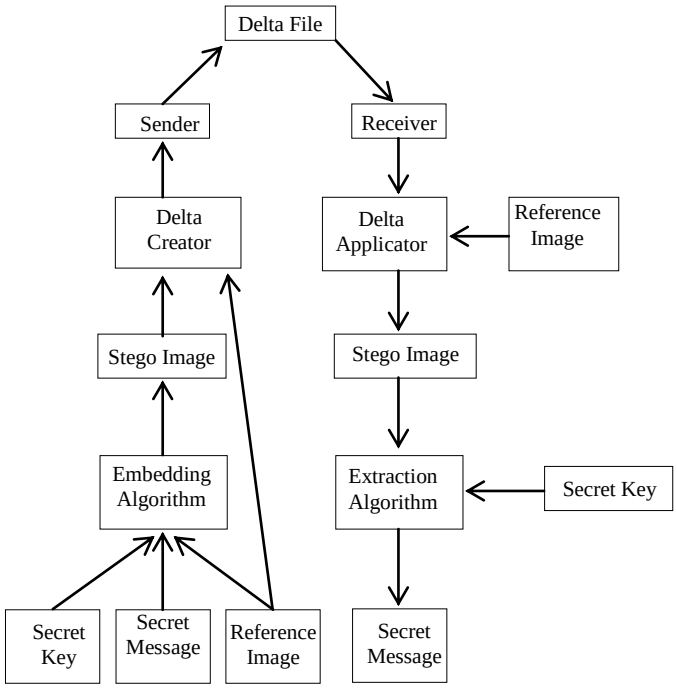


Fig. 3. The general Structure of proposed method.

V. IMPLEMENTATION

Based on the proposed algorithm, a system is developed in Java that implements the algorithm. Figure 4 shows form which has two main browsing fields. One for the secret text file to be embedded, second for the image in which to embedded the text field. After filling the necessary fields, next step enter secret key. User need not worry about the procedure behind, which in turn is automatically performed by the system itself. The secret key along with the secret message is embedded inside the image. Once the confidential data and secret key is entered, a stego image will get created and the next step is delta creation.

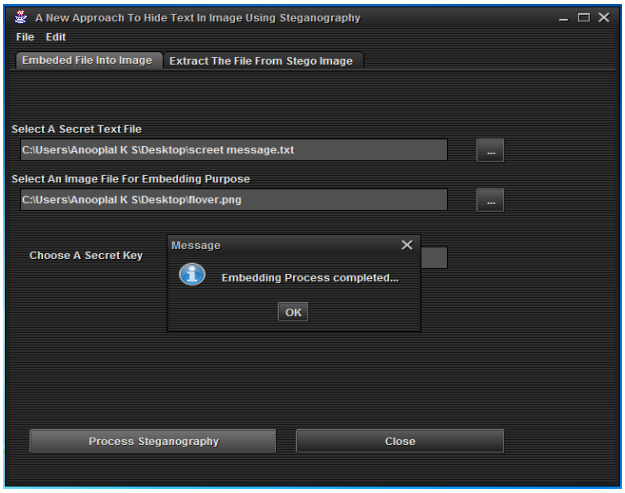


Fig. 4. Steganography Process.

The user can send this delta file to intended recipient via any communication media. Here the user sending delta file only, the reference image will be downloaded from Google or any other media without revealing the secret data. The extraction process shown in figure 5. If the intruder wants to extract the hidden data from the delta file, they need to get reference image used the similar system itself to retrieve the confidential data.

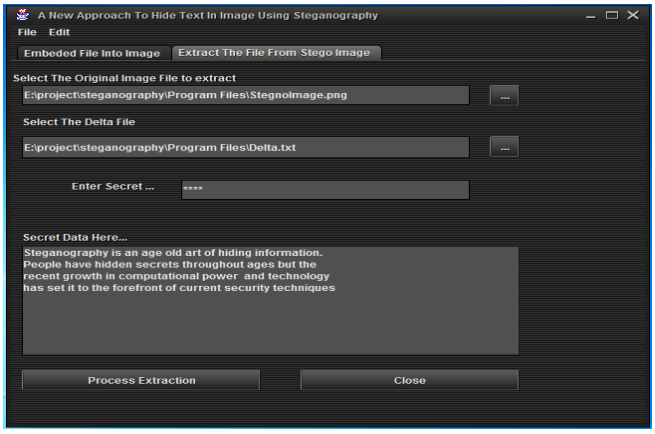


Fig. 5. Steganography Process.

VI. RESULTS

TABLE I. COMPARISON OF DIFFERENT FILE SIZES.

Sl. no	Reference image size	Text file size	Stego image size	Delta file size
1	1569KB	18KB	1519KB	191KB
2	1569KB	36KB	1701KB	323KB
3	586KB	20KB	1812KB	220KB
4	3761KB	36KB	3761KB	389KB

The system tested images and secrete messages with various sizes, the stego image doesn't have any noticeable changes, but the size of stego image is higher than reference image. The resultant delta files with various file size shown in table 1.

VII. CONCLUSION AND FUTURE WORK

This paper proposes an Infallible Method to Transfer Confidential Data Using Delta Steganography. Based on the proposed algorithm a system in Java platform is developed. Few images are tested with different size of text files to be hidden and concluded that the resulting delta file contains only the RGB value differences, the intruding person finds it difficult to interpret the contents of delta file provided he does not have the reference image and secret key. Hence this steganographic approach is robust and very efficient for hiding and transferring or storing confidential data.

During the past decade, data hiding technologies have advanced from limited use to ubiquitous deployment. With the rapid advancement of smart devices, the need to protect valuable information has generated a plethora of new methods and technologies for both good and evil. Most dangerous among these are those employ hiding methods along with cryptography, thus providing a way to both conceal the existence of hidden information while strongly protecting the information even if the channel is discovered.

REFERENCES

[1] H. Wu, H. Wang, C. Tsai and C. Wang, "Reversible image steganographic scheme via predictive coding." 1 (2010), ISSN: 01419382, pp 35-43.

[2] N. Johnson, "Survey of Steganography Software, Technical Report", January 2002.

[3] W, Peter. "Disappearing Cryptography: Information Hiding: Steganography & Watermarking" second edition. San Francisco: Morgan Kaufmann. 3(1992) pp 192-213.

[4] B. Dunbar. "A detailed look at Steganographic Techniques and their use in an Open-Systems Environment", Sans Institute, 1(2002).

[5] C. Christian. "An Information-Theoretic Model for Steganography", Proceedings of 2nd Workshop on Information Hiding, MIT Laboratory for Computer Science. 1998.

[6] Vipul Sharma and Sunny Kumar "A New Approach to Hide Text in Images Using Steganography", ISSN: 2277 128X Volume 3, Issue 4, April 2013.

[7] E. Cole, "Hiding in Plain Sight: Steganography and the Art of Covert Communication, Indianapolis", Wiley Publishing, 2003.

[8] Johnson, Neil F., "Steganography", 2000, URL: http://www.jjtc.com/stegdoc/index2.html.

[9] Johnson N.F. and Jajodia S, "Exploring steganography:Seeing the Unseen", IEEE Computer, 31(2) (1998) pp 26-34.

[10] C. H. Yang, C. Y. Weng, S. J. Wang, and H. M. Sun, "Adaptive data hiding in edge areas of images with spatialLSB domain systems," IEEE Trans. Inf. ForensicsSecurity, vol. 3, no. 3, pp. 488–497, Sep. 2008.

[11] Weiqi Luo, Fangjun Huang, and Jiwu Huang, "Edge adaptive image steganography based on LSB matching revisited," in IEEE Transactions on InformationForensics and Security, vol.5, no.2, June 2010.

[12] Provos N and Honeyman P, "Hide and seek: An introduction to steganography", IEEE Security and Privacy, 01 (3) (2003) pp 32-44.

[13] Sadkhan S.B, "Cryptography: Current status and futuretrends", Proceedings of IEEE International Conference onInformation & Communication Technologies: FromTheory to Applications, Damascus. Syria, April 19-23,2004, pp 417-418.

[13] http://www.hpl.hp.com/techreports/Compaq-DEC/WRL-97-4.pdf.

[14] http://cis.poly.edu/suel/papers/delta.pdf.

BIOGRAPHIES

[1.] **Mr. Anooplal. K. S** received B. E. Degree in Information Science & Engineering from VTU, Belgaum and pursuing M.Tech Degree in Computer Science & Engineering from Sahyadri College of Engineering & Management Mangalore, India, affiliated to Visvesvaraya Technological University (VTU) Belgaum.
Email – anooplalks@gamil.com.

[2.] **Mr. Girish. S** received B. E. in Electronics & Communication Engineering from AIT College of Engineering, Chikmagalur and M.Tech. in Networking & Internet Engineering from JNNCE, Shimoga. He is currently working as Assistant Professor in Computer Science & Engineering Department at Sahyadri College of Engineering & Management Mangalore, India-575007.
Email – giriait@gmail.com.