International Journal of Engineering Research and General Science Volume 3, Issue 4, July-August, 2015
ISSN 2091-2730

An Infallible Method to Hide Confidential Data in Video Using Delta Steganography

Anooplal. K. S, Girish. S, Arunlal. K. S

Abstract— In this modern era computers and smart devices are the major mode of communication, which connects different parts of the world within a fraction of seconds, As a result, people can easily exchange information, so that the distance is no longer a barrier for communication but safety and security may get compromised. This creates brutal issues while storing or transferring confidential data. By making use of Delta Steganography techniques, these security threats can be tackled to some extent and also eliminate unnecessary data being transmitted over network. This work introduces a combined form of steganography and delta compression algorithms. Steganography conveniently obscure confidential data inside a video file, delta compression analyze stego frames and reference frames then produce a set of instructions named as delta file. Storing or transferring delta file rather than video file can offer reduced space consumption as well as high security to the confidential data.

Keywords — Delta compression; encryption; embedding; extraction; Steganography, confidential data, stego file.

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 [1]. 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[2][3].

In steganography, before the hiding process, the sender must select a suitable shipper message, like digital file. Then select the secret message which should be in text format to embed and use an encryption key as pass phrase. A robust steganography algorithm should be selected which can encrypt or retrieve the secret message more efficiently.

The user may save or transfer the stego message to the intended receiver by using any of the modern communication technologies. The recipient after receiving the message, decrypt the hidden message using extraction algorithm with encryption key [3][7].

In this work, a secure algorithm to embed confidential data inside a video file using a new method which combines steganography technique with the support of delta compression algorithm, to get reduced space consumption as well as infallible security to the confidential data. This combination provides advantages from both algorithms like reduced file size, less band width required for transferring delta file and infallible security to the confidential data.

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.

STEGANOGRAPHY

The steganography techniques used in ancient times are generally called physical steganography. Steganography can be worn to hide confidential data intended for a specific people and also aimed to prevent the message being extracted 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 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 [1].

In this digital world, steganography methods are called digital steganography. The digital video is a moving visual images in the form of encoded digital data. Digital videos was first introduced with Sony D1 format in 1986, it measures the rate at which frames are displayed in frames per second (FPS). Since every frame is an orthogonal bitmap digital image it compares a raster of pixels. The frame rate or pixel per frame (PPF) is calculated by multiplying width (W) pixel with height (H) pixels. The color of a pixel is represented by a fixed number of bits, in RGB format contains 24 bits per pixel that is Red, Green and Blue each components contains 8 bits which means 1KB RGB image contains 341 pixels. Bits per frame (BPF) are calculated by multiplying PPF with color depth. In interlaced videos each frame is composed of two halves of an image. The first half contains only odd numbered lines of a full frame. The second half contain only even numbered lines, those halves are referred individually as fields so interlaced video has frame rate 15 FPS and field rate is 30 FPS. In compressed video each frame requires a small percentage of the original bits, that is compression algorithm shrink the input data by a compression factor. A true color video with no compression may have bits per pixel (BPP) of 24 bits / pixel. Applying jpeg compression on every frame can reduce the BPP to 16 or 12 bits/pixel. This work combines both Steganography and Delta compression methods are used to secure confidential information while storing or 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 as well as reduced file size and eliminates unnecessary data being sent over the network.

General stenographic approach is shown in figure 1. The reference message is the shipper of the secret message that may be video file. The secret message is the information which needed to be hidden in the suitable digital media and the stego video is the result of video stenographic process. The encryption key is also used while embedding the confidential data gets infallible security. The embedding algorithm is the way or idea that usually used to embed or hide the confidential information in the cover media [6] [10]. The modern steganography is also referred as digital steganography. In Digital steganography embed digital file inside other suitable digital media. Digital steganography is compared with network steganography, network steganography mask the identity information, E.g.:- in TCP/IP masking the identity information in the TCP/IP header to hide exact identity of one or more systems while secret communication [11].

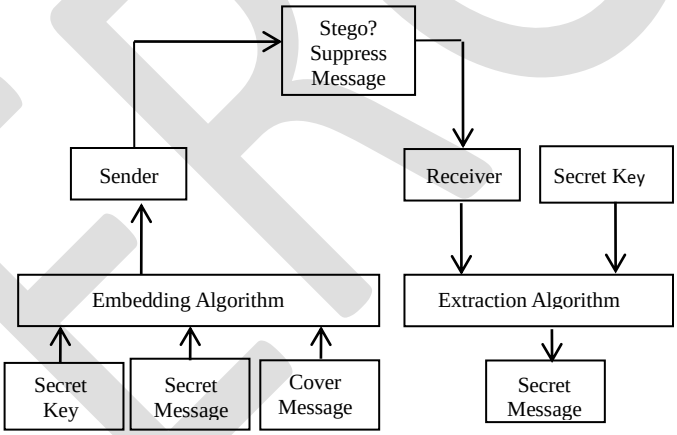


Figure. 1: General Steganography approach

DELTA COMPRESSION

In order to reduce the space consumption, to increase the efficiency of data transfers, delta compression techniques are widely used in the computer networks and in the data storage systems. Also used to eliminate unnecessary data being transmitted over network. Thus, there are many scenarios where the receiver in a data transfer already has an earlier version of the transmitted file or some other similar files are transmitted together. E.g.;-the dissemination of software packages when the receiver already has an earlier version, the transmission of relevant documents that share structure, content, or the remote synchronization of a database. In these cases, we should be able to achieve better compression than that obtained by individually compressing each file. This is the primary goal of the delta compression algorithm. Consider the case of a server distributing a software package, If the client already has an older version of the software, then a decisive dissemination scheme would only send a patch to the client that describes the differences between the old and the new version [12]. 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 stego frame, F is reference frame and ΔF is RGB difference file generally called 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

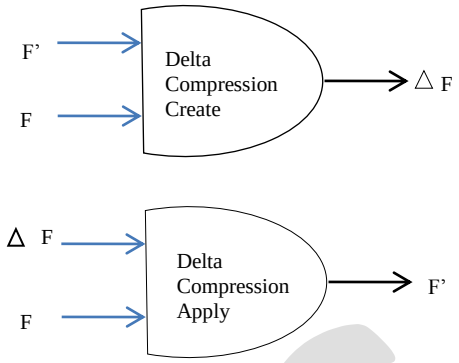


Figure. 2: Delta Compression. Size (ΔF-F') << Size (F')

PROPOSED ALGORITHM

This method resolves some of the limitations of earlier Delta Steganography technique, a more suitable approach is used for hiding the confidential data in a video. The process of hiding is explained in this section.

Calculate number of bits in confidential data and then catch first frame from the reference video file, it will be an image format then Convert frame into RGB image to get 24 bits per pixel, each color components contains 8 bits so it can hide three characters per pixel. Check if the calculated number of bits is greater than triple times of pixel density of captured frame then capture 25th frame.

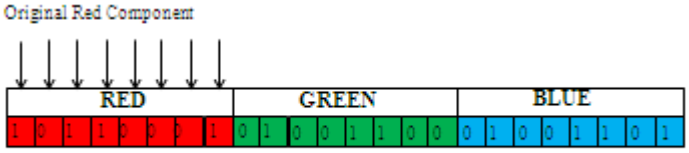
Let the data to be hidden is word "XYZ"

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

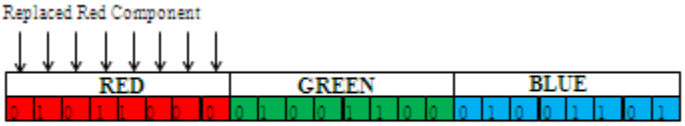
ASCII code of Y=89 and corresponding binary is 01011001.

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

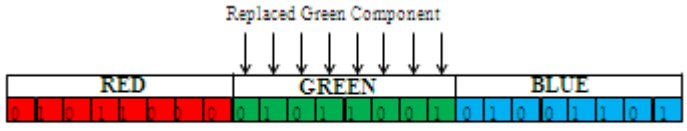
Let the RGB component of the first pixel is:-



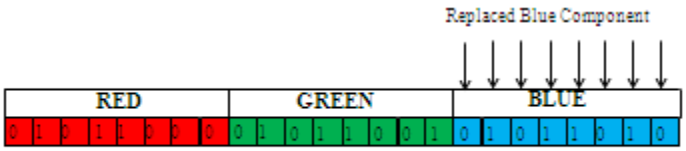
Red component is replaced with the binary of 88, i.e. X.



Replace the green component in the same pixel with binary of 89, i.e. Y.



Replace the blue component in the same pixel with binary of 90, i.e. Z.



And process continues.

Adding an encryption key to the confidential data is the first level of security. The resultant of embedding algorithm might be distorted so it may get detect if it present in video and this is the second level of security, to enhance the security of the confidential data, delta compression algorithm is used. Delta compression will compare the RGB value difference between first frame in the reference video and first frame in the stego video, also check the 25th frame in the reference video and stego video if present any changes, compare and store the instruction, all those differences into a text file named as delta file, this is the third level of security. By looking at the resulting delta file, third party cannot predict the contents inside the delta file.

The proposed steganography algorithm is a combination of embedding techniques and data extraction technique shown in figure 3. Data hiding technique as the name suggests is used to hide secret message in the video frame, while data extraction technique is used to retrieve or extract the secret message from the video frame with delta file so the confidential data is secured from unauthorized access.

THE PROPOSED EMBEDDING TECHNIQUE.

Inputs:-Confidential data, encryption key, video frames.
Output:-Delta file.

Begin

1. Select the confidential data, call ASCII code generation function.
2. Select video frames from reference video, Convert each frames into its RGB image.
3. Calculate number of bits in confidential data, Find number of pixels in frames.
4. **If** number of bits is greater than or equal to triple times of pixel density, **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 reiterate until character get empty.
   End iteration
5. Accept encryption key and call encryption.
6. Call delta creator and save delta file.

   Else
   Capture 25th frame from reference video, then go to step 2.

End

Proposed extraction technique.

Inputs:-Video frames, Encryption key, Delta file.
Output:-Confidential data.

Begin

1. Select delta file.
2. Provide encryption key and video frames, and then call extraction function.
3. Display confidential data.

End

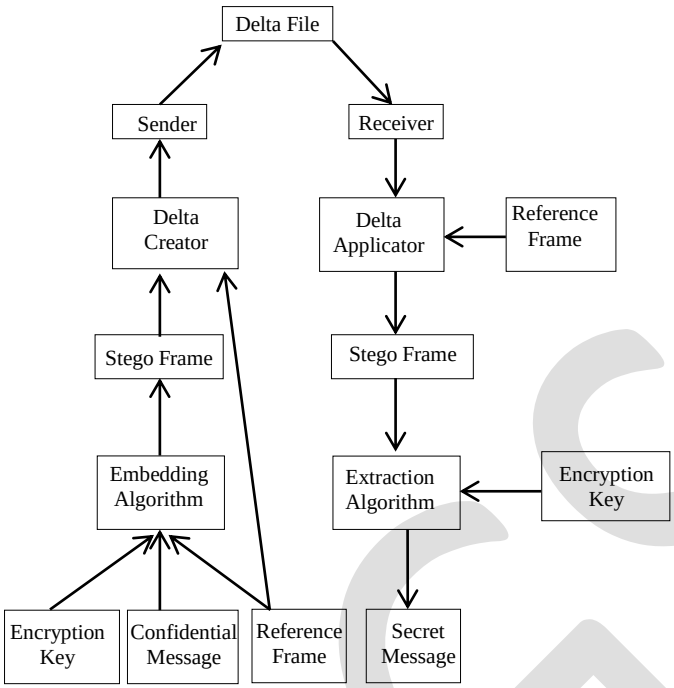


Figure. 3: The general Structure of proposed method

IMPLEMENTATION

Based on the proposed algorithms, a tool developed in Java to get object oriented features as well as security and portability to the application. The java application are interpreted so it is secure and execution under control of java virtual machine and memory allocation and reallocating done by dynamically. Figure 4 shows form which has two main browsing fields, one for the confidential data to be embedded and second for the reference video in which to embedded the secret message. After filling the mandatory fields, next footstep is enter an encryption key. End user need not worry about the procedure behind, which in turn is accordingly execute by the system itself. The encryption key along with the confidential data is embedded inside the video frame. After entering the confidential data and encryption key then click on process steganography to embed the message, shown in figure 4. After creating stego video next step is delta creation show figure 5, which compares RGB difference in both reference frames and stego frames

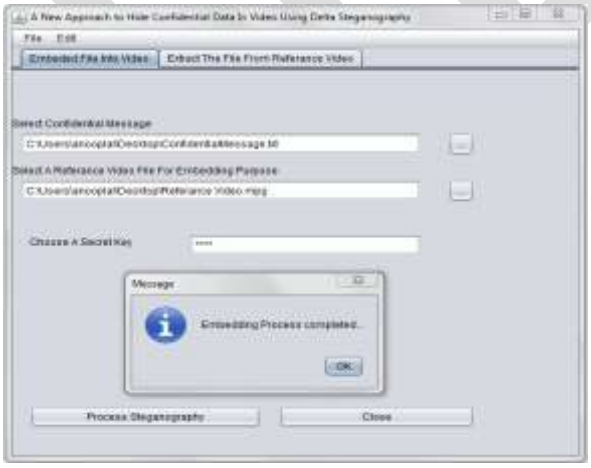


Figure. 4: Embedding Process

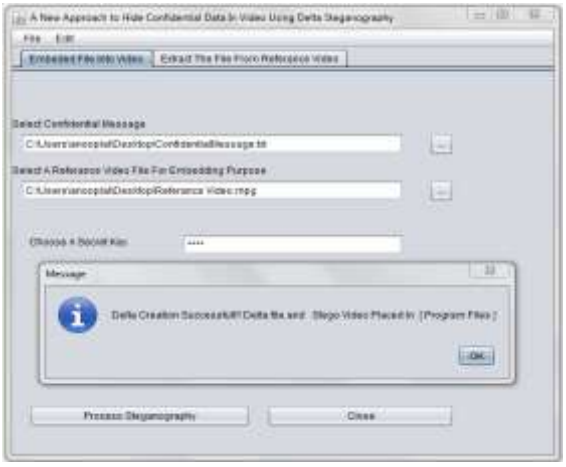


Figure. 5: Delta Creation

The user can send this delta file to intended recipient via any communication media. Here the user sending delta file only, the reference video will be downloaded from youtube or any other communication method without revealing the secret data. The extraction process shown in figure 6, if the intruder wants to extract the hidden data from the delta file, they need to get reference video used as well as same encryption key to retrieve the confidential data

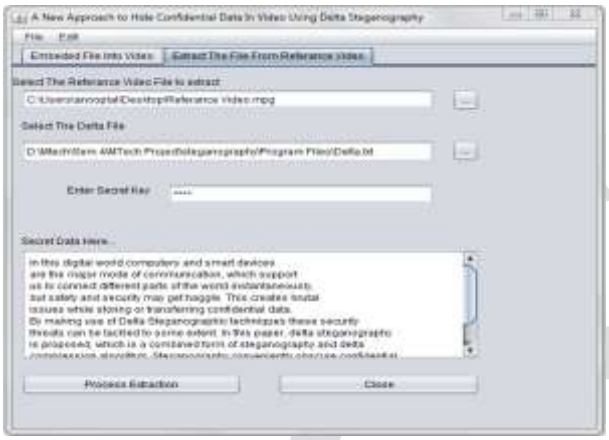


Figure. 6: Extraction Process.

RESULTS

The system tested various sized reference videos with duration 210 seconds, and confidential messages with various sizes, the stego video don't have any noticeable changes, but the size of stego video is higher than reference video. The resultant delta files shown in table 1. In addition, use any file compression utility to the delta file before transferring, it may offer one more level of security and also reduce delta file size. Using this additional feature, the eavesdropper may get confused because of delta file. Delta file contains only the RGB value differences.

TABLE 1. COMPARISON OF DIFFERENT FILE SIZES

Sl. No	Reference Video Size	Text File Size	Stego Video Size	Delta File Size
1	25767KB	60KB	32123KB	595KB
2	112560KB	20KB	119206KB	219KB
3	191940KB	28KB	199336KB	211KB
4	121590KB	64KB	124832KB	647KB
5	147630KB	28KB	156336KB	250KB

BIOGRAPHIES

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

[2.] **Mr. Girish. S** received B. E. in Electronics & Communication Engineering from VTU, Belagavi 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 Mangaluru, India-575007.Email – giriait@gmail.com.

[3.] **Mr. Arunlal. K. S** received Master of Science Degree in Electronics from M.G. University, Kottayam, Kerala and Master of Science degree in Mobile communication & Internet Technologies from Mangalore University, Mangalore. Currently working as Lecturer & Course coordinator at R. V. Centre for Cognitive Technologies Bangalore, India - 560059. Email – arunlalks1@yahoo.com

CONCLUSION

This paper described a new approach to hide confidential data in video using Delta Steganography and it is achieved by developing an algorithm in Java. Few videos are tested with different size of text files to be hidden and concluded that the resulting delta file contains only the RGB value differences between stego video frame and the reference video frame. The intruding person could not able to extract the confidential message from the delta file without reference video and encryption key. Hence this delta steganography approach is robust and high security for storing or transferring confidential data.

During the past decade, data hiding technologies have advanced from limited use to omnipresent deployment. With the breakneck 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 contribute a way to both cover up the existence of hidden information while strongly protecting the information even if the channel is discovered.

REFERENCES:

[1] Anooplal. K. S and Girish S, "An Infallible Method to Transfer Confidential Data Using Delta Steganography" International Journal of Engineering Research and Technology (IJERT) Vol.4, Issue 2, February 2015, ISSN: 2278-0181 on page(s): 1060 – 1063.

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

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

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

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

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

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

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

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

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

[11] http://en.wikipedia.org/wiki/Digital_video

[12] Torsten Suel and Nasir Memon, "Algorithms for Delta Compression and Remote File Synchronization" CIS Department Polytechnic University Brooklyn, NY 11201.

[13] R. A. Wagner and M. J. Fisher. The string-to-string correction problem. J. ACM, 21(1):168-173, January 1973.

[14] 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.

[15] 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.

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

[17] 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.

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

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