REVIEW ON VARIOUS VIDEO STEGNOGRAPHY AND COMPRESSION TECHNIQUES

Jaspreet Kaur [1], Naveen Kumari [2]

Scholar[1], Assistant Professor[2]

Department of Computer Science & Engineering , PURCITM , Mohali , Punjab

jazzrai05@yahoo.com [1] , naveencse2k4@gmail.com [2]

Abstract— The distinctive sorts of steganography are being represented considering the spread information. As the first step,the different steganography and its details are being explored. At that point, video steganography and its procedures will be explored. A few procedures including Least Significant Bits, Multiple minimum critical bits, Masking and separating and Transformations will be subjected amid picture steganography. At long last, Compression strategies will be talked about.

Keywords— video steganography ,digital message, LSB,compression,cryptography, AES

INTRODUCTION

With the development of computer and expanding its use in different areas of life and work, the issue of information security has become increasingly important. One of the grounds discussed in information security is the exchange of information through the cover media. To this end, different methods such as cryptography, steganography, coding, etc have been used. The method of steganography is among the methods that have received attention in recent years[1]. The main goal of steganography is to hide information in the other cover media so that other person will not notice the presence of the information. This is a major distinction between this method and the other methods of covert exchange of information because, for example, in cryptography, the individuals notice the information by seeing the coded information but they will not be able to comprehend the information. However, in steganography, the existence of the information in the sources will not be noticed at all [4].

Most steganography jobs have been carried out on images, video clips, texts, music and sounds .Nowadays, using a combination of steganography and the other methods, information security has improved considerably [7]. In addition to being used in the covert exchange of information, steganography is used in other grounds such as copyright, preventing e-document forging Steganography is derived from the Greek for covered writing and essentially means “to hide in plain sight”. Steganography is the art of inconspicuously hiding data within data. The main goal of steganography is to hide information well.

There are various protocols and embedding methods that enable us to conceal information in a given item [3]. In any case, the majority of the conventions and procedures must fulfill various necessities with the goal that steganography can be connected effectively.The accompanying is a rundown of fundamental prerequisites that steganography systems must fulfill:

a) The integrity of hidden data after it has been inserted inside the stego object must be redress.

b) The stego object must stay unaltered or very nearly unaltered to the naked eye.

c) In watermarking, changes in the stego object must have no impact on the watermark.

d) Finally, we generally expect that the attackers realizes that there is shrouded data inside the stego object.

Steganography differs from cryptography as in where cryptography concentrates on keeping the substance of a message mystery, steganography concentrates on keeping the presence of a message secret[5]. Steganography and cryptography are both approaches to shield data from undesirable parties yet neither innovation alone is idealize and can be traded off. Once the presence of hidden data is uncovered or even suspected, the reason for steganography is somewhat vanquished. The quality of steganography can subsequently be opened up by joining it with cryptography [14].

Two different innovations that are nearly identified with steganography are watermarking and fingerprinting [4]. These advancements are fundamentally concerned with the security of protected innovation, in this way the calculations have diverse prerequisites than steganography [13]. These necessities of a decent steganographic calculation will be talked about beneath. In watermarking the majority of the cases of an item are "checked" in the same way. The sort of data covered up in items when utilizing watermarking is generally a mark to imply cause or proprietorship with the end goal of copyright insurance.

2.Types of Steganography:

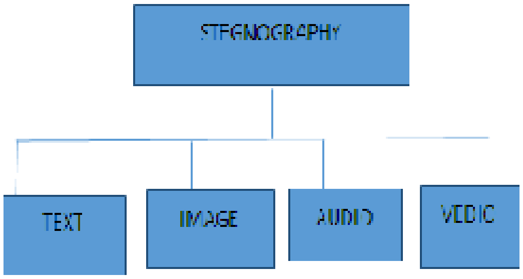

Fig. 1 Types of steganography

2.1 Text Steganography:

Hiding information in text is the most important method of steganography. The method was to hide a secret message in every nth letter of every word of a text message. After booming of Internet and different type of digital file formats it has decreased in importance. Text stenography using digital files is not used very often because the text files have a very small amount of redundant data [8].

2.2 Image Steganography:

Images are used as the popular cover objects for steganography. A message is embedded in a digital image through an embedding algorithm, using the secret key[16]. The resulting stego image is sent to the receiver. On the other side, it is processed by the extraction algorithm using the same key. During the transmission of steno image unauthenticated persons can only notice the transmission of an image but can't guess the existence of the hidden message.

2.3 Audio Steganography:

Audio stenography is masking, which exploits the properties of the human ear to hide information unnoticeably. An audible, sound can be inaudible in the presence of another louder audible sound .This property allows to select the channel in which to hide information [6].

2.4 Video Steganography:

Despite the fact that BMP documents are ideal for steganography use, they find themselves able to carry only little records [6]. So there is an issue, how to get sufficiently much documents to hide our message, and what to do to peruse them in a right request? Great way out is to conceal data in a feature record, in light of the fact that as we probably an awareness, AVI documents are made out of bitmaps, consolidated into one piece, which are played in right request and with appropriate time gap. Remembering that we should simply to get out is record single casings and spare them as BMP records [11]. In the event that we'll utilize calculation for hiding information in advanced pictures, we can conceal our message in bitmap acquired along these lines, and afterward spare it into new AVI record.

We'll use uncompressed AVI document, in light of the fact that if any pressure is executed records loses its information. AVI documents are made out of couple streams. Essential record stream is a feature stream and sound stream, which can be document of any expansion, for example WAVE. Due to presence of those streams, it is conceivable to hide information in document's casings as well as in specified sound stream [6]. On account of this we can consolidate chances of concealing information in advanced pictures.

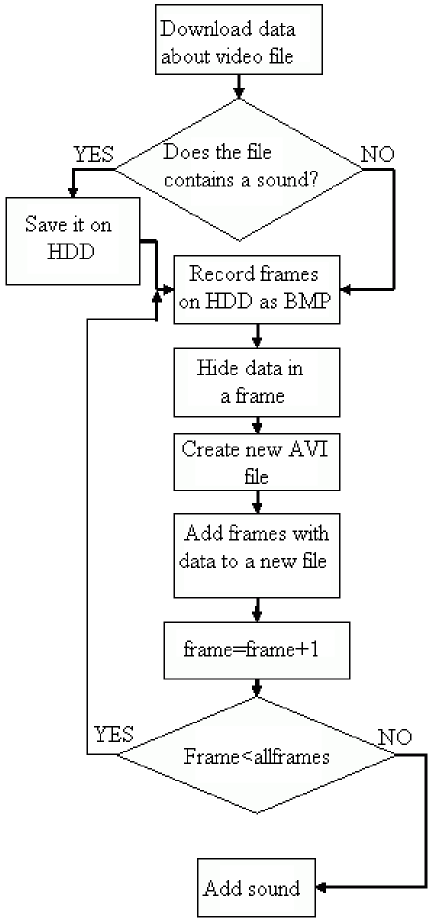
Download data about video file
Does the file contains a sound?
YES
NO
Save it on HDD
Record frames on HDD as BMP
Hide data in a frame
Create new AVI file
Add frames with data to a new file
frame=frame+1
YES
Frame<allframes
NO
Add sound

Fig 2 Working of videoSteganography

3.Steganography Techniques

3.1 Physical

Steganography has been generally utilized, incorporating in late authentic times and the present day. Known cases incorporate like Hidden messages inside wax tables — in old Greece, individuals composed messages on the wood, then secured it with wax whereupon a guiltless covering message was composed [6]. Second are Hidden messages on ambassador's body — additionally utilized as a part of old Greece. Herodotus recounts the narrative of a message tattooed on the shaved leader of a slave of Histiaeus, covered up by the hair that thereafter developed over it, and uncovered by shaving the head once more. The message purportedly conveyed a notice to Greece about Persian attack arranges. This technique has evident downsides, for example, deferred transmission while sitting tight for the slave's hair to develop, and the limitations on the number and size of messages that can be encoded on one individual's scalp.

3.2 Digital messages

Current steganography entered the world in 1985 with the appearance of the PCs being connected to traditional steganography issues [6]. Advancement taking after that was moderate, yet has following taken off, passing by the substantial number of steganography programming accessible: Concealing messages inside the most minimal bits of uproarious pictures or sound records. Covering information inside scrambled information or inside irregular information. The information to be disguised are initially encoded before being utilized to overwrite a piece of a much bigger square of scrambled information or a square of arbitrary information.

3.3 Digital content

Making content the same shading as the foundation in word processor archives, messages, and discussion posts. Utilizing Unicode characters that resemble the standard ASCII character set [3]. On most frameworks, there is no visual distinction from normal content. A few frameworks may show the textual styles in an unexpected way, and the additional data would be effortlessly spotted.

3.4 Social Steganography

In groups with social or government taboos or restriction, individuals use social steganography: concealing messages in saying, popular society references, and different messages that are imparted freely and thought to be observed [3]. This depends on social setting to make the basic messages obvious just to specific peruses Examples include: Hiding a message in the title and connection of an imparted feature or picture

3.5 Network

All data concealing systems that may be utilized to trade steganograms in telecom systems can be arranged under the general term of system steganography. This terminology was initially presented by Krzyszt of Szczypiorski in 2003[2]. In spite of the common steganography systems which use computerized media (pictures, sound and feature records) as a spread for shrouded information, system steganography uses correspondence conventions' control components and their essential inborn usefulness. Subsequently, such strategies are harder to recognize and dispense with.

3.6 Printed

Advanced steganography yield may be as printed records. A message, the plaintext, may be initially encoded by conventional means, delivering a figure content. At that point, a harmless spread content is changed somehow in order to contain the figure content, bringing about the stego content. Case in point, [2] the letter size, separating, typeface, or different attributes of a spread content can be controlled to convey the shrouded message. Just a beneficiary who knows the procedure utilized can recoup the message and afterward decode it [3]. Francis Bacon built up Bacon's figure all things considered a met

4. Applications of Steganography

Steganography is appropriate to, yet not constrained to, the accompanying regions.

1) Confidential correspondence and mystery information putting away.

2) Protection of information modification.

3) Access control framework for advanced substance circulation.

4) Media Database frameworks.

4.1 Confidential correspondence and mystery information putting away

The "mystery" of the implanted information is fundamental around there. Verifiably, steganography have been drawn closer around there. Steganography furnishes us with:

(A) Potential ability to shroud the presence of private information

(B) Hardness of identifying the shrouded (i.e., installed) information

(C) Strengthening of the mystery of the encoded information

By and by, when you utilize some steganography, you should first choose a vessel information as per the span of the implanting information. The vessel ought to be harmless. At that point, you insert the private information by utilizing an installing system (which is one segment of the steganography programming) together with some key. At the point when separating, you (or your gathering) utilize an extricating project (another part) to recoup the installed information by the same key ("basic key" as far as cryptography) [3]. For this situation you require a "key arrangement" before you begin correspondence. Joining a stego document to an email message is the most straightforward sample in this application territory. However, you and your gathering must do a "sending-and-getting" activity that could be recognized by an outsider. Thus, messaging is not a totally mystery specialized system. There is a simple strategy that has no key-arrangement. We have a model of "Unknown Covert Mailing System." [6] .Each mystery based application needs an installing procedure which leaves the littlest implanting proof. You may take after the accompanying.

(A) Choose a huge vessel, bigger the better, contrasted and the inserting information.

(B) Discard the first vessel in the wake of inserting.

4.2 Security of information change

We exploit the delicacy of the inserted information in this application region. We stated in the Home Page that "the inserted information can preferably be delicate than be extremely hearty." Actually, installed information are delicate in most steganography projects. Particularly, Qtech Hide & View project installs information in an amazingly delicate way. We exhibit this in the other page. Be that as it may, this delicacy opens another heading toward a data change defensive framework, for example, a "Computerized Certificate Document System." [13] The most novel point among others is that "no confirmation department is required." If it is actualized, individuals can send their "advanced declaration information" to wherever on the planet through Internet [7]. Nobody can fashion, adjust, nor alter such authentication information. On the off chance that produced, modified, or altered, it is effortlessly distinguished by the extraction program. Simply visit this page and see the reference

4.3.Access control system for digital content distribution

Around there inserted information is "shrouded", however is "clarified" to announce the substance. Today, computerized substance are getting more regularly conveyed over Internet than anytime recently. For instance, music organizations discharge new collections on their Webpage in a free or charged way. Nonetheless, for this situation, all the substance are just as appropriated to the individuals who can make access to the page. In this way, a conventional Web dispersion plan is not suited for a "case-by-case" and "particular" circulation. Obviously it is constantly conceivable to append computerized substance to email messages and send them to the clients. Be that as it may, it will takes a considerable measure of expense in time and work [7] . In the event that you have some profitable substance, which you think it is distributable in the event that somebody truly needs it, and in the event that it is conceivable to transfer that substance on Internet in some secret way. We have added to a model of an "Entrance Control System" for computerized substance dispersion through Internet. The accompanying steps clarify the plan.

(1) A substance proprietor group his/her advanced substance in an envelope by-organizer way, and implant the entire organizers in some substantial vessel as indicated by a steganographic technique utilizing organizer access keys, and transfer the implanted vessel (stego information) on his/her own Webpage[15].

(2) On that Webpage the proprietor clarifies the substance top to bottom and expose around the world. The contact data to the proprietor (post mail address, email location, telephone number, and so on.) will be posted there.

(3) The proprietor may get an entrance demand from a client who viewed that Webpage. All things considered, the proprietor may (or may not) makes an entrance key and give it to the client (free or charged).

4.4 Media Database frameworks

In this application territory of steganography mystery is not vital, but rather binding together two sorts of information into one is the most imperative [14]. Media information (photograph picture, film, music, and so on.) have some relationship with other data. A photograph picture, for case, may have the accompanying.

(1) The title of the photo and some physical article data

(2) The date and the time when the photo was taken

(3) The cam and the picture taker's data

5. Approaches used

5.1 LSB (Least significant Bit)

Least significant bit (LSB) is the bit position in a binaryinteger giving the units value, that is, determining whether the number is even or odd. The LSB is sometimes referred to as the right-most bit, due to the convention in positional notation of writing less significant digit further to the right[9]. It is analogous to the least significant digit of a decimal integer, which is the digit in the ones (right-most) positioned and Technology.

5.2 AES

The Advanced Encryption Standard (AES) is a specification for theencryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.AES is based on the Rijndael cipher developed by two Belgiancryptographers, Joan Daemen and Vincent Rijmen, who submitted a proposal to NIST during the AES selection process[6]. Rijndael is a group of figures with distinctive key and piece sizes.For AES, NIST chose three individuals from the Rijndael family, each with a square size of 128 bits, yet three diverse key lengths: 128, 192 and 256 bits.AES has been received by the U.S. government and is currently utilized around the world. It supersedes the Data Encryption Standard (DES) [7], which was distributed in 1977. The calculation depicted by AES is a symmetric-key calculation, significance the same key is utilized for both encoding and decoding the information.

REFERENCES:

[1] Getup, A. "Pixel Indicator Technique for RGB Image Steganography" *Journal of Emerging Technologies in Web Intelligence, 2010,* Vol. 2, pp. 193-198.

[2] Marwaha, P. "Visual cryptographic Steganography in images"*Second International conference on Computing, Communication and Networking Technologies,2010***,** pp. 34-39.

[3] Bailey, K. "An evaluation of image based Steganography methods"*Journal of Multimedia Tools and Applications, 2006*,Vol. 30**,** pp. 55-88.

[4] Mahata, S.K. "A Novel Approach of Steganography using Hill Cipher" *International Conference on Computing, Communication and Sensor Network (CCSN), 2012,* pp. 0975-888.

[5] Chapman, M. Davida G, and Rennhard M. "A Practical and Effective Approach to Large Scale Automated Linguistic Steganography"found online at

[6] Mehboob, B. "A Steganography implementation"*International Symposium on Biometrics and Security Technologies, 2008*, pp.1 – 5.

[7] Saravanan, V. "Security issues in computer networks and Steganography"*7th International Conference on* Intelligent Systems and Control (ISCO), 2013 , pp. 363 – 366.

[8] Moon, S.K. "Data Security Using Data Hiding"*International Conference on Computational Intelligence and Multimedia Applications, 2007,* pp. 247 – 251.

[9] Mr .VikasTyagi, Mr. Atulkumar Roshan Patel3, SachinTyagi, Saurabh Singh Gangwar,"image steganography using least significant bit with cryptography" Journal of Global Research in Computer Science,Volume 3, No. 3, March 2012,pp 53-55.

[10] Swati malik, Ajit "Securing Data by Using Cryptography with Steganography" International Journal ofAdvanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013

[11] Ishwarjot Singh „J.P Raina,“ Advance Scheme for Secret Data Hiding System using Hop field & LSB" InternationalJournal of Computer Trends and Technology (IJCTT) – volume 4 Issue 7–July 2013.

[12] G. Manikandan, N. Sairam and M. Kamarasan "A Hybrid Approach for Security Enhancement by CompressedCrypto-Stegno Scheme ", Research Journal of Applied Sciences, Engineering and Technology 4(6): 608-614, 2012

[13] Shabir A. Parah, Javaid A. Sheikh, G.M. Bhat, "Data Hiding in Intermediate Significant Bit Planes, A HighCapacity Blind Steganographic Technique", International Conference on Emerging Trends in Science,Engineering and Technology , pp.192-197, July 2012.

[14] Michel K. Kulhandjian, Dimitris A. Pados, Ming Li, Stella N. Batalama, and Michael J. Medley, "Extractingspread-spectrum hidden data from digital media ", IEEE transactions on information forensics and security, vol. 8,no. 7, july 2013.

[15] Chang, Chin-Chen., Lin, Iuan-Chang., and Yaun-Hui YU., " A new Steganographic method for color and grayscale image hiding", Computer Vision and Image Understanding, ELSEVIER, Vol. 107, No. 3, pp. 183-194,2007.

[16] Bailey, K., and Curran, K., "An Evaluation of Image Based Steganography Methods", Journal of Multimedia Toolsand

Applications, Vol. 30, No. 1, pp. 55-88, 2006