Globus An International Journal of Management & IT
A Refereed Research Journal
Vol 10 / No 2 / Jan-Jun 2019 ISSN: 0975-721X

A STEGANOGRAPHY TECHNIQUE BASED ON MULTIPLE-IMAGE INTERFERENCE

*Apoorva Sharma
** Upendra Rawat
***Dr. Naveen Tyagi

Abstract

Steganography is the science of camouflaging message, video, image or any other data within another file, which can be any multimedia file. The purpose of this technique is to hide the existence of the message in cover file from unauthorized party. It takes the advantages of limited perception of human to observe subtle changes in images, sound etc. Here our concern is about digital images as they are more frequent over the internet. In spy/hacker world Steganography and Cryptography are cousins. Cryptography alters a message so it cannot be understood whereas Steganography hides the message so that it cannot be read. An approach for Steganography Technique Based on multiple-image Interference and position multiplexing is proposed based on the interference principle.

Keywords: Authenticity, mesh network, roaming protocols, security attacks, handoff.

Introduction

The ability to protect sagacious information from adversary, principally during their transmission through channels that are disparate to have leaks, is vital in a world of promising cyber war. Nowadays, each and every one electronic message is being constantly and without human intervention monitored by both private and state-owned intelligent systems that have an enormous computer power [2]. In particular, every transmission of cipher-text calls the attention of any of these systems and unquestionably is chosen to be analyzed, among others, by competitors and any sort of divergent forces. The use of electronic transmission media requires a method that calls less attention of the managerial automatic systems. Recent Steganography offers an intensity of examine that includes privacy, integrity ,authenticity, and confidentiality of the transmitted records

The majority image steganographic algorithms implement an presented image as a cover medium to hide a secret message. The disbursement of embedding secret messages into this swathe image is the image misrepresentation encountered in the stego image. This leads to two complication. First, since the dimension of the cover image is fixed, the more secret messages which are embedded permit for more image distortion. Therefore, a compromise has to be reached between the embedding capability and the image excellence which consequences in the limited capacity provided in a few definite cover images[14], evoke that image steganalysis is an approach used to sense secret messages hidden in the stego image. A stego image has some alteration, and in spite of how minute it is, this will hold up with the normal features of the cover image[10]. This leads to the another drawback for the reason that it is still probable that an image steganalytic algorithm can conquer the image steganography and thus disclose that a hidden message is being conveyed in a stego image.

The paper is organized as follows. In section II, we discuss about the system model, followed by the discussion on the security issues and analysis in

**M.Tech Scholar, Department of Computer Science and Engineering, MIT, Bulandshahr*
*** Assistant Professor, Department of Computer Science and Engineering, MIT, Bulandshahr*
****Professor, Department of Computer Science and Engineering, MIT, Bulandshahr*

section III. Proposed stegnography model. Finally, in Section IV, we conclude the paper, and references are given at the end of the paper.

System Model

In the available stegnography algorithms if someone have image and key then extract message by the available image stegnography process

If anyone wishes to hide any message in an image with a key but wish that no one extract that message even if have key and image both. We explain an example of bank locker. Where as a locker have a pair of keys. In bank, a locker is open by pair of keys one is customer key and another manager key.

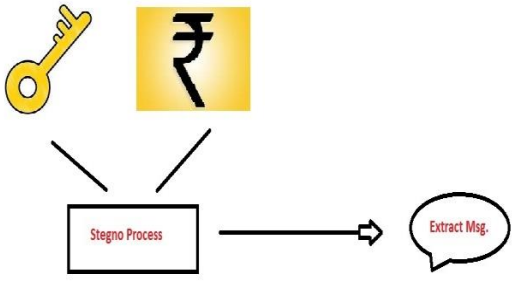

Fig.1 Stegno Process

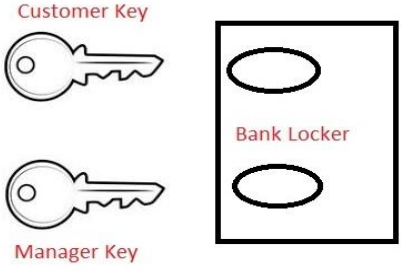

Fig. 2 Bank Locker Open System

In bank if anyone wants to open locker then required both customer key and manger key. If there is only one key present then it is impossible to open locker.

We proposed a stegnography algorithm in which use interference of multiple images with the same shared key and secret message. In Proposed stegnography algorithm distribute secret message among multiple images and by the use of shared key create multiple stegno images. If anyone wishes that no one extract that message even if have key and image both.

A grain synthesis procedure re-samples a diminutive grain image drawn by an artist or captured in a photograph in order to create a new grain image with a similar local emergence and capricious size[12]. We intertwine the grain creation process into steganography concealing secret messages as well as the source grain. In particular, in compare to using a presented cover image to hide messages, our algorithm conceals the source texture image and embeds secret messages in the course of the process of grain synthesis. This permit we to pull out the secret messages and the source grain from a stego synthetic grain. To the superlative of our understanding, steganography delightful benefit of the reversibility has constantly been obtainable within the literature of grain synthesis.

The message pull out for the receiver side involves generating the manifestation table, retrieving the source grain, performing the grain synthesis, and extracting and authenticating the secret message masked in the stego synthetic grain.

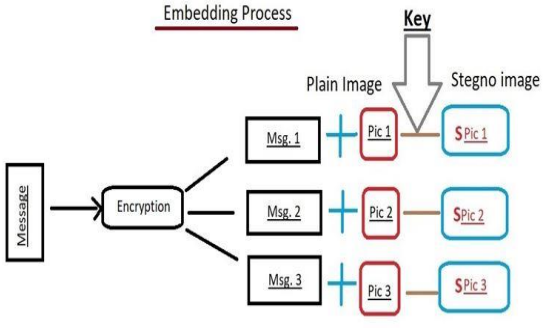

Fig. 3 Extraction algorithm describe in Embedded Algorithm

Proposed Model

(A) Proposed Embedded Algorithm

We propose a stegnography approach in which use interference of multiple images to hide the same message, proposed approach work as a function which take message and a key to hide a message in multiple images at receiver end.

g (msg, key, n*img)

Where g is stegno function take three arguments msg., key and multiple images.

The Embedding process describe

Embedded Algorithm

1. Embedding (Msg, Key, N_Imgs)
2. Input Msg, Key and N no. of Imgs.
3. ploy_encr(Msg, Key)
   return encrypted data
4. Split encrypted data into N unit n1, n2….n
5. Each data unit embedded with an image by use secret Key
6. Return embedded images

(B) Proposed Extraction Algorithm

Extracting Algorithm

1. Extracting (N_Imgs, Key)
2. Input N no. of Imgs. In same sequence and Key
3. Encrypted Data extracted from each embedded image by use secret Key.
4. Merge extracted data as D
5. ploy_decr(D, Key)
   Return decrypted data
6. Return extracted hide message

Fig. 3.2 Extraction algorithm describe in Embedded

In extraction process take multiple images in the same SEQUENCE as the time of EMBEDDIND OF MESSAGE , it first extract the hidden message by the use of shared secret key then merge the all parts of extracted hidden message and perform decryption on the message call decryption algorithm now return the plain text message as result.

Conclusion

In this paper, Data confidentiality protects encryption of data but it is not adequate. We take the benefits of stegnography with cryptography, where no one knows that what data is transfer. Stegnography hide the secret message in a stegno object. In this thesis, a new stegnography method uses in this proposed method multiple images uses rather than uses a single image with a shared secret key.

As the secret message embedded in multiple images after encryption by shared key then embedded images distributed in individuals so no one can extract the secret hide message even if have both key and image. This proposed approach implemented successfully in MATLAB where we use three images to hide a secret message.

There is no conciliation with the quality of stego-image that is cover image and secret message. The quality of stego-image is 100% conserved in this method. The stego image create by process is visually impossible to differentiate from the cover image and there is no distortion in extracted message.

We studied the various authentication schemes that have evolved over a decade. They cater to the requirements of authentication in different areas of wireless networks. In table 1, we compared the various proposed cellular network authentication schemes during hand-off process based on scalability, anonymity etc. and also addressed the authentication schemes of other areas in wireless networks at various layers of OSI model such as in mesh networks, sensor networks, vehicular communication etc. these authentication schemes not only provide the authentication as well as also provide the additional security from a variety of threats.

References

1. T. Morkel , J.H.P. Eloff and M.S. Olivier “An Overview of Image Steganography”.
2. Amanpreet Kaur, Renu Dhir, and Geeta Sikka “A New Image Steganography Based On First Component Alteration Technique” (IJCSIS) International Journal of Computer Science and Information Security,Vol. 6, No. 3, 2009.
3. Nagham Hamid, Abid Yahya, R. Badlishah Ahmad and Osamah M. Al-Qershi “ImageSteganography Techniques: An Overview” International Journal of Computer Science and Security (IJCSS), Volume (6): Issue (3): 2013.
4. A. Soria, R. Cumbrera, and Y. Fonseca, “Steganographic algorithm of private key on the domain of the cosine discrete transform,” Revista Cubana de Ciencias Inform´aticas, vol. 10, no. 2, pp. 116–131, 2016.
5. Volume 4, Issue 1, January 2014 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering Research Paper Available online at: www.ijarcsse.com An Overview of Different Type of Data Hiding Scheme in Image using Steganographic Techniques Mukesh Garg* A.P. Gurudev Jangra M.Tech. Scholar H.O.D in CSE Department Jind Institute of Engineering & Technology Jind Institute of Engineering & Technology Jind,

Haryana 126102, India Jind, Haryana 126102, India.
6. Sarreshtedari Saeed & Mohammad Ali Akhaee. (2013). One-third probability embedding: a new ±1 histogram compensating image least significant bit steganography scheme, Journal on IET Image Processing.
7. Chang, Chin-Chen & Hsien-Wen Tseng. (2009). Data hiding in images by hybrid LSB substitution. Third International Conference on. IEEE Multimedia and Ubiquitous Engineering, China.
8. Zhang, Jun, Feng Xiong & Dan Zhang. (2012). Steganalysis for LSB Matching Based on the Dependences Between Neighboring Pixels. Journal of Multimedia.
9. V.M Potdar & E. Chang. (2004). Grey level modification steganography for secret communication. IEEE Conference on Industrial Informatics, Berlin.
10. MA Khan, V Potdar & E Chang. (2004). An architecture platform for grey level modification steganography system IEEE Industrial Electronics Society, South Korea.
11. Feng, Pan. Jun Li, Xiuguang Li & Yao Guo. (2011). Steganography based on Minimizing Embedding Impact function and HVS. IEEE International Conference on Electronics Communications and Control (ICECC), Ningbo. China.
12. Ki-Hyun Jung & Kee-Young Yoo. (2014). Directional Data Hiding Method for Digital Images, Cryptologia.
13. Lee CF, Chen HL & Tso HK. (2010). Embedding capacity raising in reversible data hiding based on prediction of difference expansion. Journal of Systems and Software.
14. Wenbo Zhou, Weiming Zhang & Nenghai Yu. (2017). A New rule for cost reassignment in adaptive steganography. IEEE transactions on information forensics and security.
15. Chuan Qin, Chin-Chen Chang & Tai-Jung Hsu. (2014). Reversible data hiding scheme based on exploiting modification direction with two steganographic images. Springer Science and Business Media, New York.
16. Lee CF, Chen HL & Tso HK. (2010). Embedding capacity raising in reversible data hiding based on prediction of difference expansion. Journal of Systems and Software.