Global Journals LaTeX JournalKaleidoscope™

Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

Chaotic Sequence based Steganography for Pair-Wise Communication

Harsha S[1], Shailesh Kumar[2], Dr. Khalid Nazim Sattar Abdus[3], Dr. Keshava Prasanna[4] and Shantanu Agara Dwarakanath[5]

[1] Visvesvaraya Technological Univeristy

Received: 7 December 2015 Accepted: 3 January 2016 Published: 15 January 2016

Abstract

Steganography is the art and science of hiding sensitive data inside an image. There are so many cryptosystems that use Steganography as a major tool. Also in recent years there is a rising trend towards chaotic sequence based cryptosystems. This paper attempts to combine the two with a new algorithm for data hiding. Here key images required for Steganography are generated using chaotic sequence. Also an attempt is made to overcome the limitations of Steganography on the file size ratio and the security offered by Steganography.

Index terms— steganography, chaotic sequence, data hiding, PRNG.

1 Introduction

teganography refers to covered writing [1]. Digital images, videos or files can be used as cover to hide the message that has to be communicated. Steganography is different from Cryptography. Cryptography involves encryption which is scrambling the information in a systematic way that renders the message unintelligible, whereas Steganography is information hiding using basic Boolean operations inside an image, video or another file [3]. Steganography is the art and science of communicating in a way which hides the existence of the communication. In contrast to cryptography, where the enemy is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second secret message present [4]. This is where Steganography comes in. Unlike cryptography, the purpose of Steganography is to hide a message. All Steganography requires is a cover text, which is where data will be hidden, a message that is made up of data, an algorithm that decides how to hide the data, and frequently, a key that will be used to randomize the placement of the data and perhaps even encrypt it.

Steganography has its own limitations [1]. They are as follows;

? The file size ratio of Key and plain text has to be >=8:1. ? The only bit altered is the least significant bit [2] of each byte making it easy to crack. ? The images that are used for key are not completely offline and many are easily available.

In this paper we have made an attempt to overcome the said limitations of Steganography by developing a new algorithm.

2 II.

3 Methodology

Our proposed algorithm is developed in two phases.

4 Phase 1: Key generation

Here images having chaotic number sequences for pixels are generated according to the user requirement. In the experimentation such a generation of 10 images with 600X800 pixels is shown. Each pixel is having 24 bit depth indicating 1 byte per colour in the R-G-B palette [5]. The images are numbered sequentially. This number forms another key for pair-wise encryption.

5 Phase 2: Encryption/Decryption

The plain text file [6] inclusive of the header is converted into a bit stream. This is ex-ored with the selected image using the hop length selected by the user. The hop length is the third key towards enhancing the security offered by the proposed system. For decryption the new image generated will be ex-ored with

6 E

The basic idea behind cryptography is that one can keep a message a secret by encoding it so that no one can read it. If a good cryptographic cipher is used, it is likely that no one, not even a government entity, will be able to read it. However, sometimes merely communicating in secret can trip up alarms and make others suspicious. This is where cryptography fails. While it may very well be unbreakable by all available standards, an encrypted message is easy to detect and flag as secret [1]. the original image. The result will be written into a file which would be the plain text file that was hidden.

The idea here is to avoid using publicly available or regular images. For this system to work, we propose a new system of images that use a chaotic sequence for hiding the information.

7 III.

8 Implementation

The implementation of our system is divided into 4 modules. Module 1. Image generation: Here a simple program is used to generate the key images. The images are bitmaps (.bmp) having dimensions of 600X800 pixels. The entire image will be a chaotic sequence of numbers. Hence the image looks like noise as shown in Fig. **??**. First the image header is written into a key file having 53 bytes (for .bmp format). Then the pixels are loaded with 24 bit random numbers that make up Red, Green and Blue coloursin each pixel. Module 2. Image exchange module: In this module the images generated are exchanged between the pair of users as the title suggests. Each time a pair of users decides to use this system, before communication they use the image generation module and exchange the images. The image set can be exchanged physically/offline or online via a secure channel. In this paper we have generated 10 images per set and 6 possible hop lengths per image. So, each set can be used for 60 independent communications between the pair. Module 3. Encryption Module: This module is built to hide the data inside the chaotic image. Here a bitwise EXOR operation is done with the bits from the information (plain text) file and the key file. The advantage of the proposed system is evident here. In Steganography the file size is limited by the ratio 8:1. Where as in our system, each bit in a pixel can be altered without changing the appearance of the key file. This is due to the random nature of the key image files. Also for large files, multiple images can be used in sequence or if the file size is not an integral multiple of the hop count, the same image can be used in a cyclic repetitive fashion for data hiding. Module 4. Decryption Module: In this module the image received (containing the hidden message) is first used to get the key image ID and the hop count. Then it is exored with the key image file in the image set having the same ID and the bits at the hop count are written into a file. This file forms the decrypted message.

IV.

9 Experimentation and Results

Fig. **??** : A sample of generated image using chaotic sequence for pixels.

As shown in Fig. **??**. A set of images are generated and then used for hiding different types of files. The key images and the images with hidden data are shown in Fig. **??**.1 through 2.10. Due to the randomness in the image the hidden message will be rendered invisible to the naked eye as well as computer programs. This image is then embedded with the key file ID and the hop count using the file footer system or any available data embedding system such as water marking at the pixel level or salt and pepper data hiding method **??**7][8]. This is left to the user to choose. Or the user may choose to communicate the key file ID and hop count in a separate message using a different hand-shake method. Once the data (plain text) is hidden in the key file, it can be sent in any open channel. Also as an added measure, the key image after the data hiding operation can be given a new extension (.DUS (Data Under Steganography or. VE (Visual Encryption) [9]) to avoid most operating systems from attempting to open it.

It can be clearly seen from Fig. **??**.1 through 2.10 that there is visibly no way to cryptanalyse the cipher text without access to the original key image set. Even then the attacker needs the hop count as the image can be used in a cyclic fashion. When analysed with available cryptanalysis methods, Brute force method known as Dictionary attack [10] yields parts of the plain text in 7.7176X10 23 using the formula Cryptanalysis time T c =2 L where L=Key length in bits.

(1) The analysis also indicates that the system is breakable if the attacker has copies of all communications and by happenstance obtains the same key image used repeatedly [11]. The occurrence of this demands that the attacker monitors each and every communication between the pair of users. Hence the possibility of the system

being cracked is very low. The regression analysis shows that the relevance between Plain text and Cipher text for a 1 kB text file is less than 0.18 using the Pearson Product moment correlation [12]. This shows that a simple backtracking method will not succeed in breaking our method. V.

10 Conclusion

From our work it can be concluded that, Steganography, even though shunned as old, can be altered to prove very useful **??**13]. The tweaks and added features that we have shown in this paper make sure that the communication is safe and secure if only the pair of users can maintain the key files are safe and offline all the time. Thus our proposed system works better on any type of file with any operating system. It fares well against most of the known cryptanalysis methods. Hence it proves to be an efficient and universal steganographic system for individual as well as organizational users for pair wise communication. This also opens up a line of research for developing methods based on our work to have the following features

? Larger key sets with verifiable randomness ? Sequential steganpgraphy of larger files using multiple key images ? Design and development of a server to function as arbitrator of generalised system, to overcome the limitation of pair wise communication.

11 References Références Referencias

2016

Figure 1: S © 2016

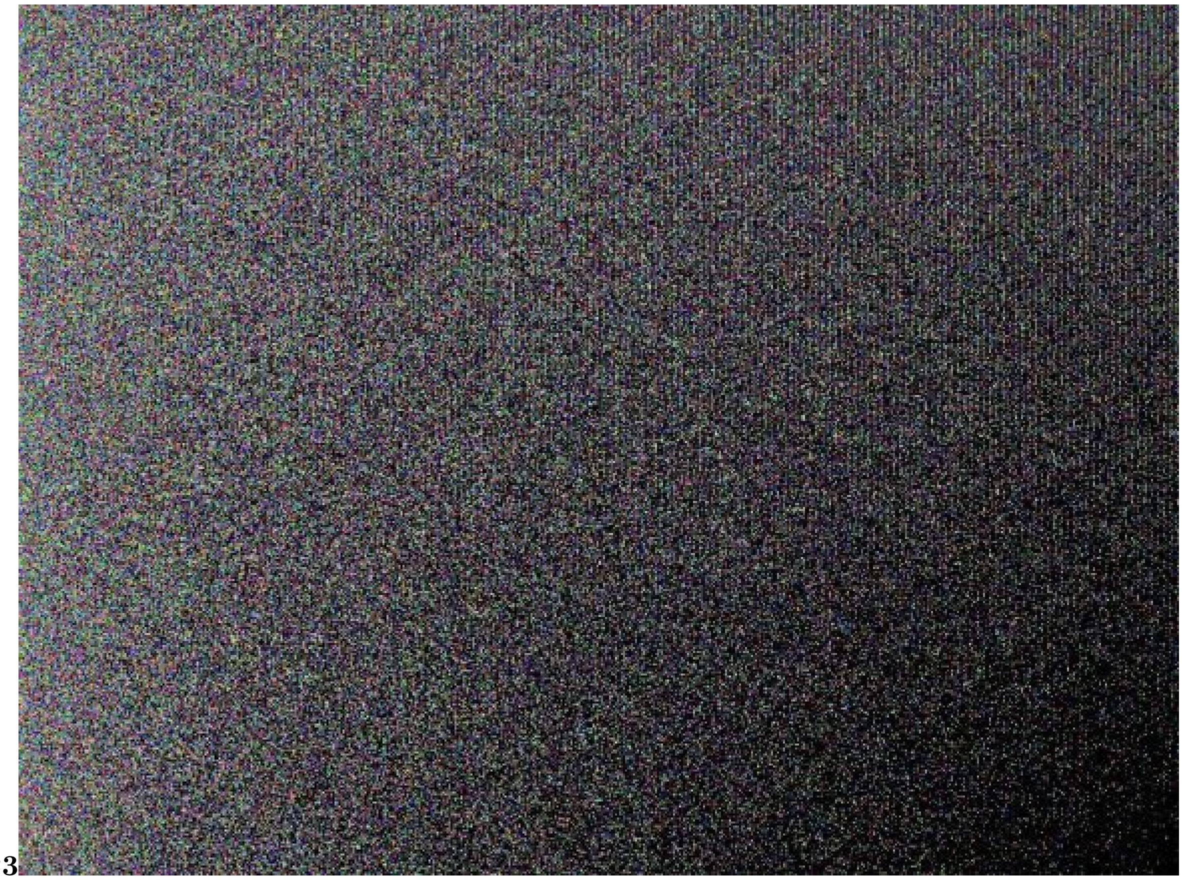
212112223

Figure 2: Fig. 2 . 1 :Fig. 2 . 1 :Image 1 Fig. 2 . 2 :Fig. 2 . 3 :

2642842729210

Figure 3: Fig. 2 . 6 :Image 4 Fig. 2 . 8 :Image 4 Fig. 2 . 7 :Fig. 2 . 9 :Fig 2 . 10 :


Steganography is the art and science of hiding sensitive data inside an image. There are so many cryptosystems that use Steganography as a major tool. Also in recent years there is a rising trend towards chaotic sequence based cryptosystems. This paper attempts to combine the two with a new algorithm for data hiding. Here key images required for Steganography are generated using chaotic sequence. Also an attempt is made to overcome the limitations of Steganography on the file size ratio and the security offered by Steganography.

Figure 4:

[Shareza Shirali ()] 'A new Approach to Persian/Arabic Text Stegraphy'. M Shareza Shirali . *Computer and Information Science* 2006, ICISCOMSAR 2006. p. 5.

[Chang and Lin (2006)] 'A new Steganographic method for color and gray scale image hiding'. Chin-Chen Chang , Iuan-Chang Lin , Yaun-Hui , YU . *Computer Vision and Image Understanding*, 20 December 2006.

[Chapman and Davida ()] *A Practical and Effective Approach to Large-Scale Automated Linguistic Steganography*, M Chapman , G Davida , RennhardM . http://www.nicetext.com/doc/isc01.pdf 2003.

[Bailey and Curran ()] 'An evaluation of imagebased steganography methods'. K Bailey , K Curran . *International Journal of Digital Evidence* 2003.

[Gujarati and Econometrics ()] 'Combination of Cyphertext and Audio Steganography Technique for Secrete Communication'. Damodar Gujarati , Basic Econometrics . *International Journal of Emerging Technology and Advanced Engineering* 2250- 2459. 2003 13. December 2012. McGraw-Hill Publications. 2 (12) . (Budda Lavanya, Vittapu Sravan kumar)

[Digital Watermarking for Digital Media, Information Science Publishing] http://www.igi-global.com/chapter/digital-watermarking-multim-edia-trans-action-tracking/8553 *Digital Watermarking for Digital Media, Information Science Publishing*,

[Cole ()] *Hiding in Plain Sight: Steganography and the Art of Covert Communication*, Eric Cole . 2003. Wiley.

[IEEE/ACIS International Conference (2006)] *IEEE/ACIS International Conference*, July 2006. p. .

[Fabien ()] *Information Hiding: Techniques for Steganography and Digital Watermarking*, A P Fabien , Petitcolas . 2000. Boston: Artech House. p. .

[Johnson and Doric ()] Neil F Johnson , Doric . *Zoran / Jajodia Information Hiding: Steganography and Watermarking Attacks and Countermeasures*, (U.S.A.) 2001. Springer. 1. (Advances in Information Security)

[Anderson and Petitcolas ()] 'On the Limits of steganography'. R J Anderson , F A P Petitcolas . *Selected Areas in Communication*, 1998. 16 p. .

[Dai and Liu (2006)] 'Predictive-CodingBased Steganography and Modification for Enhanced Security'. Y Dai , G Liu , Wangz . *IJCSNS International Journal of Computer Science and Network Security* March 2006. 6 (3b) .

[Steganography: Hidden Data. Quick study by Deborah Radcliff Computerworld] 'Steganography: Hidden Data. Quick study by Deborah Radcliff'. http://www.computerworld.com/securitytopics/security/story/0 *Computerworld*