International Journal of Control Theory and Applications

ISSN : 0974–5572

Volume 9 • Number 42 • 2016

Steganography Based Remote user Authentication System

Srinidhi G.A[a] and K.B. ShivaKumar[b]

[a]*Research Scholar, Sri Siddhartha Academy of Higher Education, Tumakuru Karnataka, India*

E-mail: srinidhiga@ssit.edu.in

[b]*Research Supervisor, Sri Siddhartha Academy of Higher Education, Tumakuru*

E-mail: shivakumarkb@ssit.edu.in

Abstract: With the rapid use of the networks for authentication for various applications like authorized access, Money transactions etc has made life very easy and comfortable. This has achieved a true freedom from hard core documentation and rapid use of hard copies which has a limited life time. At the same time this method of using the digital data has led us to face a lot of problems like eavesdropping the authenticated data, unintended access for many facilities etc. This paper provides a new scheme to have a protected authentication for facilities by using the trending technology called steganography. Here the user's photograph which has to be authenticated remotely will be embedded into a simple cover image which inturn remains as it was earlier and doesn't even give a simple clue about the presence of covert data. This scheme is said to be easily usable as it has been coded to have a simple GUI which can be easily used by a common layman.

Keyword: *Steganography, Watermarking, remote user authentication.*

1. INTRODUCTION

The word has become a global village. The process of transferring the information from one place to another across the world has become a simple game of the figure tip. The advancement in technology has made all these things possible and as eased the life of every individual. Each and every process such as a simple application for the use of government facilities, government jobs, application for a valid identity card etc and most complex and important processes such as having a financial transaction authenticated, remote access to most important facilities like printers of currency notes etc has become digitized. We can have a simple android based mobile phone using which authentication for a most important facility can be easily created. We have to make a note that this simple handheld device will be connected to most complicated internet which is being used by many individuals in the world using different gateways equipped with different levels of security restrictions. Once the data is over the net, we will be unable to trace who will be using the data and from which part of the world.

This problem has been the most debated research topic in both industry and academia. Many different algorithms has been proposed and are available in the literature. These algorithms can be classified into three different technologies namely 1. Cryptography 2. Watermarking 3. Steganography. The earlier two technologies are said to give the eavesdropper that something is present in the data which makes him to think about decoding the data. If these decoding techniques are working, then there is no chance for the data being protected.

Steganography is a new scheme which may be considered as the improved version of cryptography. Here the result of the embedding process hides the existence of the covert data itself. Stego images are considered to be easily uploaded into social media as well as it will easily hide the existence of the data itself. At the receiver end the covert data can be easily extracted using the reverse process of embedding so that the secret data will in the hands of an authenticated user or the system.

Now a days in telecommunications industry, the issue of the Subscriber Identity modules (SIM) are taking place through a small mobile retailers who were earlier collecting the data of the subscriber as a hardcopy such as passport size photographs, an identity card issued by the government authority etc and were issuing the SIM cards which were getting activated after the documents being verified. Now a days there has been a rapid use of technology where these SIM cards are being issued based on the digital data where the photograph of the subscriber will be clicked by the retailer and will be uploaded into the website of the mobile service provider. This process will have a danger where these photographs may be hacked easily and may be used to activate those SIM cards which may be further used for illegal activities.

This process proposed scheme uses steganography and puts forth a new algorithm which provides a solution for the above discussed problems.

This article has been divided into different parts. Part one introduces and defines the intended problem, part two discusses and comments about the existing algorithms and systems as available in the literature. Third section gives details about the proposed scheme whereas the fourth part provides the snap shots developed GUIs under the title results. The paper will be concluded with final conclusions.

The algorithm gives a better solution for the problem discussed and hopefully will be useful for the common man. Page Layout

2. EXISTING SYSTEM

Klimis Ntalianis and Nicolas Tsapatsoulis [1] proposed an authentication scheme using semantic segmentation, chaotic cipher text generation scheme and steganography. Here if a user wills to remotely authenticate some data, then a video object is segmented using an automatic algorithm by employing a head- and- body detector. Further, the user's any of the biometric signal is used to generate cipher data by employing chaotic cipher. This encrypted information is embedded into the most significant wavelet coefficient of the video object using QSWT which serves with both invisibility and significant resistance against lossy transmission and compression which are quite common in the unsecured public transmission channel like internet. To compare with the other existing algorithms, it has an advantage that the compression of the signal after encryption, makes it good. Therefore, the scheme can be used further to have data hiding which becomes a strong algorithm. Steganography along with an encryption algorithm makes an algorithm always strong.Xinyi

Zhou et al., [2] proposed a method for LSB steganography combining it with cryptography which is applied on to color images where secret key for encryption is also being used. The information hiding and cryptography has been combined together which increases the human eye visual features and the identity authentication based on digital signature. The encryption employed here makes it more secured and strong algorithm. Weiming Zhang et al., [3] proposed a scheme for non adaptive distortion steganography by defining joint distortion on pixel blocks. The joint distortion has been decomposed into distortion on individual pixels has been employed so as to reduce the complexity for minimizing joint distortion so that the data can be embedded with syndrome trellis codes.

Pascal Schöttle and Rainer Böhme [4] proposed a model which had a equilibrium in mixed strategies, which is based on the heterogeneity of the cover source. Adding realism by employing imperfect recoverability of the adaptivity criterion and prove that naïve adaptive embedding—the strategy implemented in a number of practical schemes—is only optimal if perfect steganography is possible or if the adaptivity criterion is not recoverable at all. In practice, where steganography is imperfect and adaptivity criteria are partially recoverable, the optimal embedding strategy is between naïve adaptive and random uniform embedding.

Guanshuo Xu et al., [5] reported a CNN architecture that takes into account knowledge of steganalysis. In the detailed architecture, taking absolute values of elements in the feature maps generated from the first convolutional layer to facilitate and improve statistical modeling in the subsequent layers; to prevent overfitting, Constrain the range of data values with the saturation regions of hyperbolic tangent (TanH) at early stages of the networks and reduce the strength of modeling using 1 × 1 convolutions in deeper layers. Although it learns from only one type of noise residual, the proposed CNN is competitive in terms of detection performance compared with the SRM with ensemble classifiers on the BOSSbase for detecting S-UNIWARD and HILL. Jiang Yu et al., [6] proposed a scheme for spatial steganalysis based on contrast of residuals (CoR). After selecting complex blocks froman uncompressed image by a fluctuation function, the residuals are calculated from the selected blocks and the whole image after applying diverse filters. The CoR is represented as an angle and the norm of residuals is considered as the corresponding weight of angle, which is used as the new steganalysis feature. In their proposed scheme, no quantization and truncation is required and the effective information of long-range dependencies among pixels is kept properly. Also, the dimensionality of feature is linear with the number of residuals. The accuracy of scheme is evaluated on HUGO and WOW algorithms.

Weiming Zhang et al.,[7] proposed a framework for non-additive distortion steganography by defining joint distortion on pixel blocks. To reduce the complexity for minimizing joint distortion, we design an coding method to decompose the joint distortion (abbreviated to DeJoin) into distortion on individual pixels and thus the message can be efficiently embedded with syndrome trellis codes (STCs)

3. PROPOSED MODEL

As dicussed the system has been proposed as a solution to the problem as mentioned in the introduction part. Here the major agenda is to protect the subscriber data. The over all block diagram of the system is as shown in figure 1:

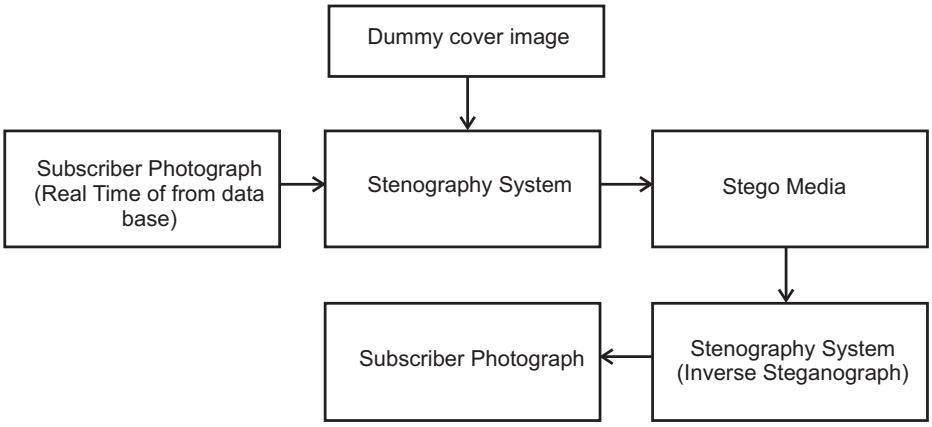

Figure 1: Over all block Diagram of the proposed system

As shown in figure 1 the very basic step of the algorithm is to have an option for the user to have the data being read into the system either by using the builtin camera of the computer system or by using the existing images which are readily available in the system.

The next stage is to have the steganography system which is going to use the very basic LSB steganography which is a very simple algorithm which generates a stego media which can be easily transmitted using any of the transmitting media like email attachment, can be posted in a social media etc.

At the receiver end the receiver will simply download the snapshot and using the inverse of the steganography scheme, the payload data can be easily decoded.

4. SIMULATION RESULTS

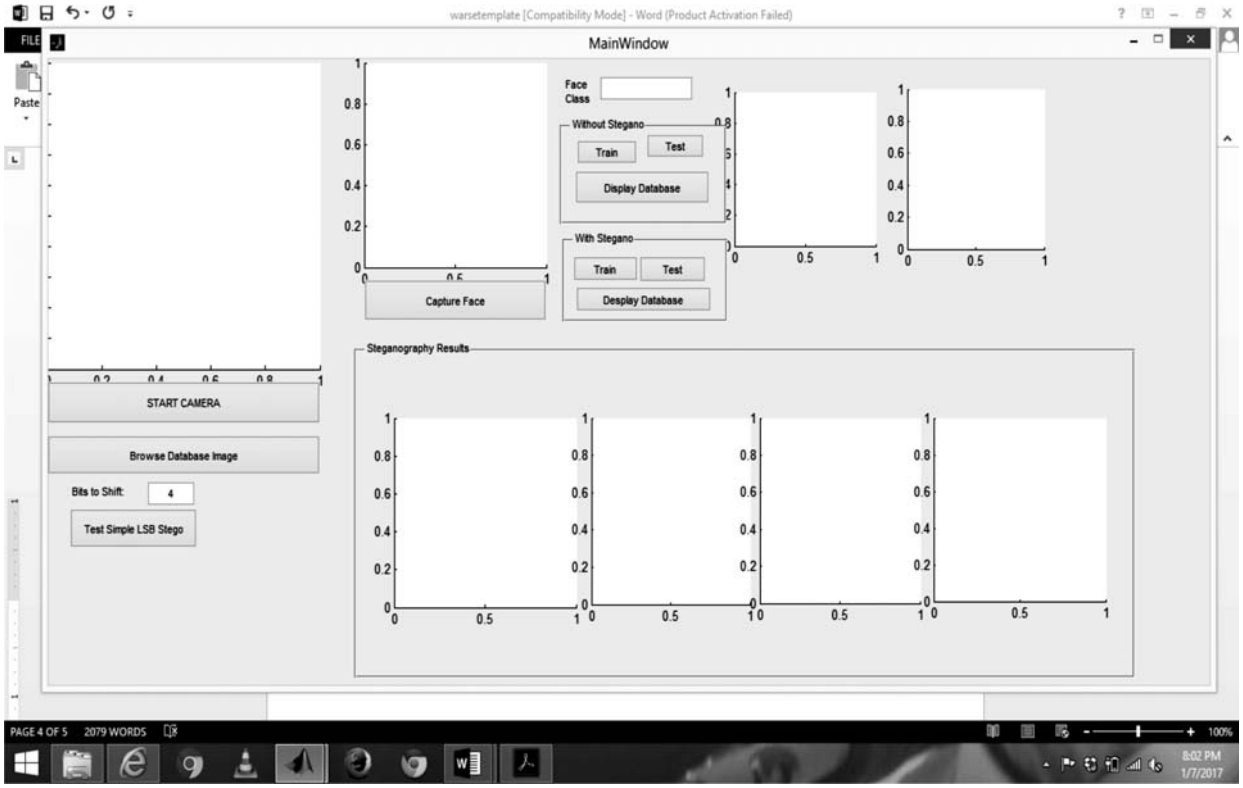

Figure 2: Developed GUI to test different image

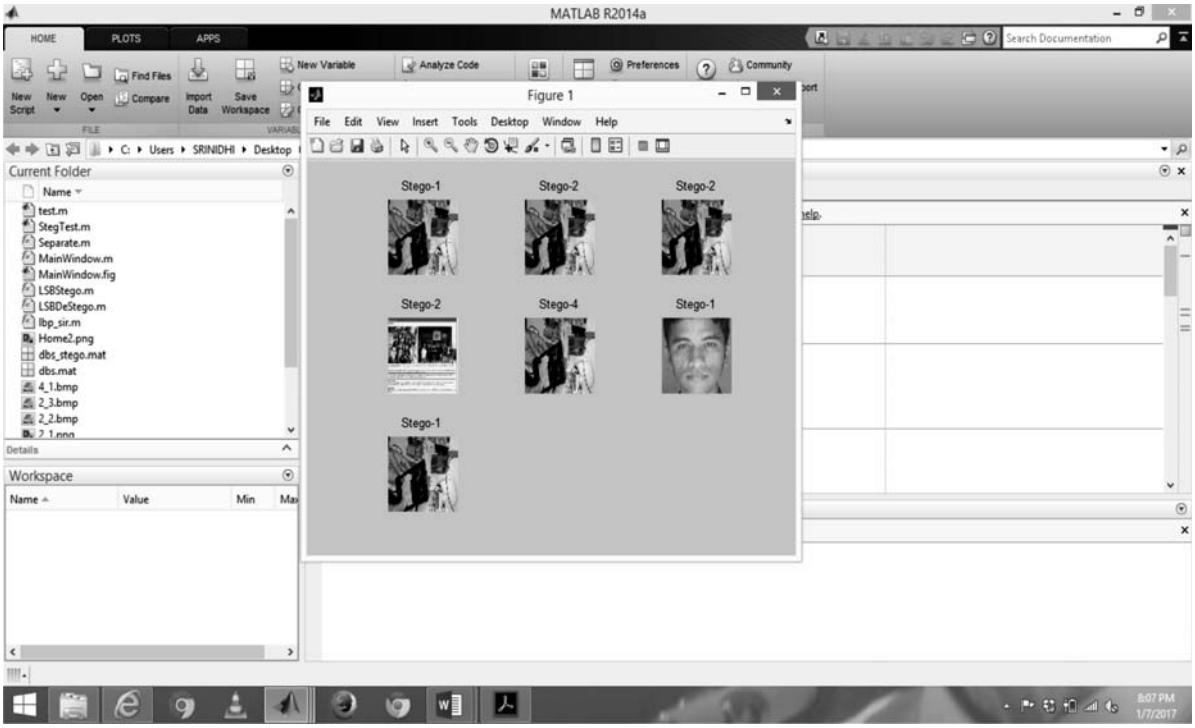

Figure 3: Screen shot showing different stego images used for testing

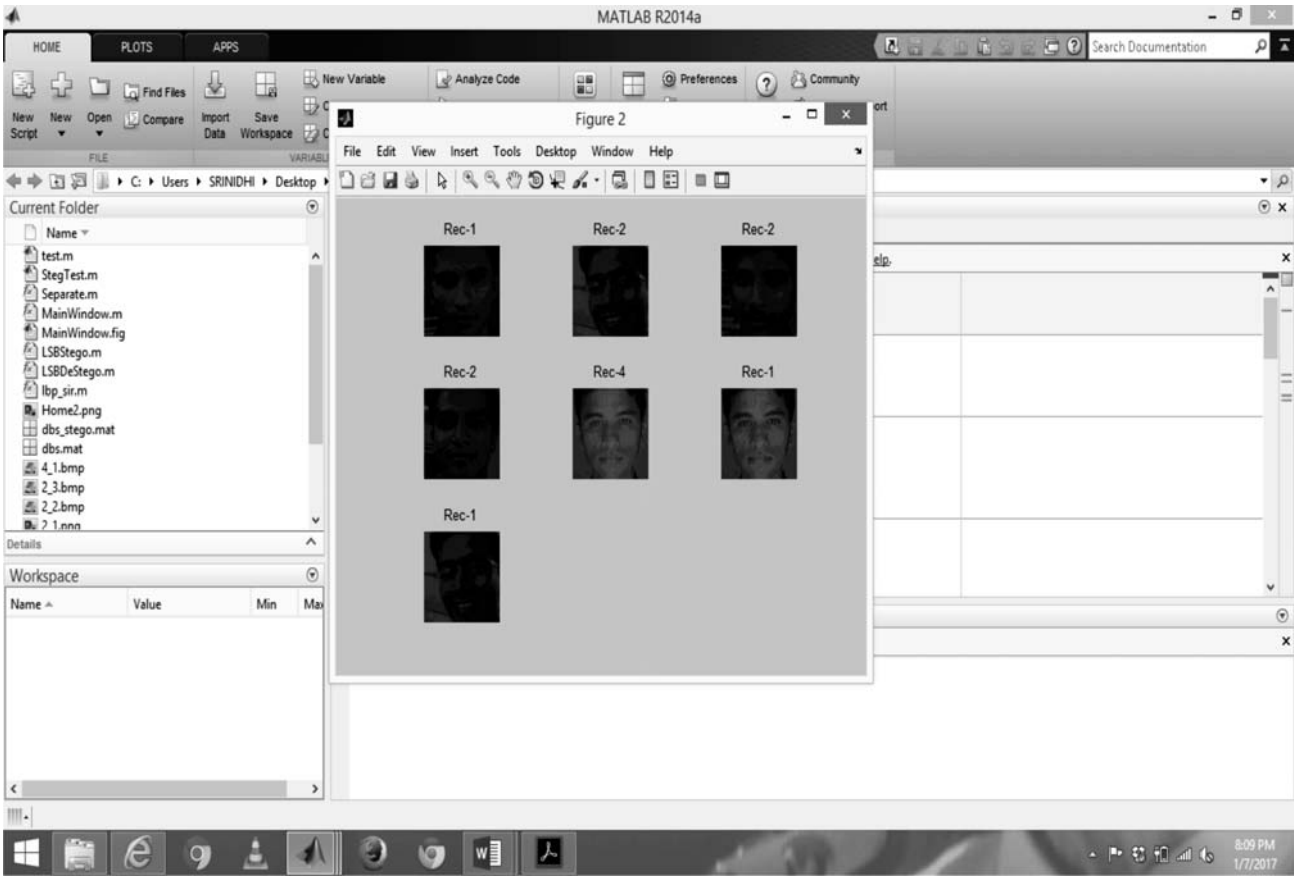

Figure 4: Decrypted Payload at the destination

5. CONCLUSIONS

As per the requirement of the day, many biometric signals is being frequently used particularly in the field of authentication. Therefore the proposed system is said to be serving the purpose. Here the most discussed field of information hiding *i.e.*, Steganography has been used which makes it advantageous and is being used to serve the purpose. This makes the algorithm technically strong. The simulation tool has been used to develop a simple GUI which makes it very simple to use and understand the algorithm.

This algorithm will be further tested with various parameters of steganography like PSNR and hiding capacity. It is hoped that the results of this testing will be quite promising as we have considered all the parameters of information hiding while designing the algorithm.

REFERENCES

[1] Klimis Ntalianis and Nicolas Tsapatsoulis, "Remote Authentication via Biometrics: A Robust Video-Object Steganographic Mechanism Over Wireless Networks," IEEE Transactions on Emerging Topics in Computing, Vol 4, No 1, pp: 156-174, March 2016.

[2] Xinyi Zhou, Wei Gong, WenLong Fu and LiaJing Jin, "An Improved Methos for LSB Based Color Image Steganography Combined with Cryptography," ICIS, June 2016.

[3] Weiming Zhang, Zhuo Zhang, Lili Zhang, Hanyi Li and Nenghai Yu, "Decomposing Joint Distortion for Adaptive Steganography," IEEE Transactions on Circuits and Systems for Video Technology, pp:1-7, 2016.

[4] Pascal Schöttle and Rainer Böhme, "Game Theory and Adaptive Steganography," IEEE Transactions On Information Forensics And Security, Vol. 11, No. 4, April 2016.

[5] Guanshuo Xu, Han-Zhou Wu, and Yun-Qing Shi, "Structural Design of Convolutional Neural Networks for Steganalysis," IEEE Signal Processing Letters, Vol. 23, No. 5, May 2016

[6] Jiang Yu, Fengyong Li, Hang Cheng, and Xinpeng Zhang, "Spatial Steganalysis Using Contrast of Residuals," IEEE Signal Processing Letters, Vol. 23, No. 7, July 2016

[7] Weiming Zhang, Zhuo Zhang, Lili Zhang, Hanyi Li and Nenghai Yu, "Decomposing Joint Distortion for Adaptive Steganography," IEEE Transactions on Circuits and Systems for Video Technology, 2016.