American Journal of Advanced Research, 2018, 2–1
December. 2018, pages 31-34
doi: 10.5281/zenodo.1439330
http://www.ibii-us.org/Journals/AJAR/
ISBN 2472-9264 (Online), 2472-9256 (Print)

Short Communication

Secured Online Transcript Issuing and Processing Using Crypto-Steganography Technique

Bamidele Ibitayo Faluyi[1,*], Ogunlola Okunola Olasunkanmi[1], Ayodele, Olukemi Sade[2]

[1]Department of Computer Science, Federal Polytechnic, Ado-Ekiti, Nigeria,
[2]Department of Computer Science, Kogi State Polytechnic, Lokoja, Kogi State, Nigeria

*dele.faluyi@yahoo.com

Received on May 16, 2018; revised on September 26, 2018; published on September 30, 2018

Abstract

Confidentiality and accuracy are two prime concerns of issuers of academic history of any tertiary institution to students, otherwise known as transcript, which in most cases are sacrificed for timeliness of its availability for the purpose of its request. Most Nigerian graduates have forfeited great opportunities that come their ways as a result of late arrival of their transcripts to the requesting agents. In this paper, we propose a processing of online request and sending of academic history to and fro requesting agents and sending institutions using Crypto-steganography which is a combination of Cryptography and Steganography methods of securing information. RSA algorithm was used in the Cryptography module Hash-LSB technique was adopted in the Steganography module. With this approach, confidentiality of the document is ensured while the receiving agents also receive the document in good time. Unified Modeling Language was used as design tool while Javafx was used to implement the scheme.

Keywords: *Steganography, Cryptography, Confidentiality, Transcript*

1 Introduction

Transcript is documentation of a student's permanent academic record, which usually means all courses taken, all grades received, all honors received and degrees conferred to a student. In the internet age, all our daily life actions have been managed electronically using huge number of computers connected by internet network. These electronic actions include e-commerce, online banking, online booking of air flight tickets, students registering in the tertiary institutions and online applying for visa. All these activities need to produce and manage documents digitally, an example on these documents, including university transcripts, letters and business contracts (Fischer and Herfet, 2006; Abboud, 2015). Producing digital documents electronically is more suitable and simpler than paper documents and also dealing with paperless documents is far better because of the ease of editing, searching and storing of them (Fischer *et al*, 2007; Abboud, 2015). In addition, making these documents available digitally in the computer networks permit them to be transmitted and processed electronically (Fischer and Herfet, 2006). However, releasing documents in the networks exposes them to different types of attacks, hackers and threats, hence; protecting digital documents is very significant matter in the networked society (Abboud, 2015). The releasing documents has to be secured using the combination of cryptography and steganography to secure it. In this present digital development, it is very difficult to deliver private information on a communication network in a safe and secured manner. Therefore, a secret communication is required to protect the information from third party attackers which is the difficult challenge of information security. Several methods have been proposed for addressing the issue of information security like cryptography and steganography. Cryptography encrypt information in such form that it becomes meaningless to eavesdroppers using any encryption algorithms (Singh, 2017).

Cryptography is a technique in which original data (Plaintext) is converted to some unreadable form of data (Cipher text) with help of some secret key using some ciphering algorithm. Steganography is a practice of secret communication of data. In Cryptography, secret message is kept in an unreadable format to a third person, while in steganography method existence of secret message is hidden from the third person. In Steganography technique, sender sends a message by hiding it within some multimedia data like text, image, audio or video (Trivedi and Rana, 2017). Although both cryptography and steganography try to protect data, but neither technology alone is perfect but it is better to combine both approaches together to increase the information security and to increase the degree of security of the system (Mercuri, 2004; Singh, 2017). But in cryptography its always clear to intermediary person that the message is in encrypted form whereas in steganography the secret message is made to hide in cover image so that it could not be clearer to any hacker that whether there is any message hidden in the information being shared. The cover image containing the secret message is then transferred to the recipient. The recipient is able to extract the message with the help of retrieving process and secret key provided by the sender. The Figure 1 below show the combination of cryptography with steganography process (Halder *et al*., 2016).

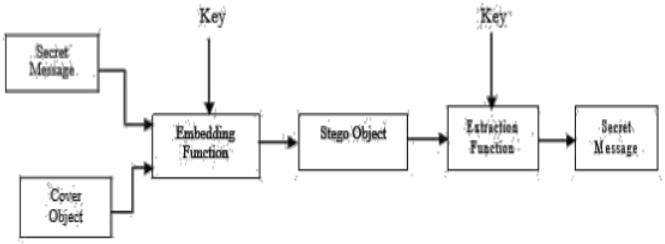

Figure 1: Combination of Cryptography with Steganography (Halder *et al.*, 2016)

Steganography has multiple fields of use, but the classic field of use for steganography is hidden communication. For example, Alice needs to send a message to Bob through a stego-channel that is monitored by a warden. The warden reads all the messages before they arrive to Bob. In cases when the warden finds something suspicious the message is blocked and will never reach Bob. Figure 2 represents hidden communication. In such a situation, cryptography will protect the message itself, but will raise the suspicion of the warden. Steganography would embed the secret message into another message or an image and the warden would ideally let it through to Bob without any suspicion.

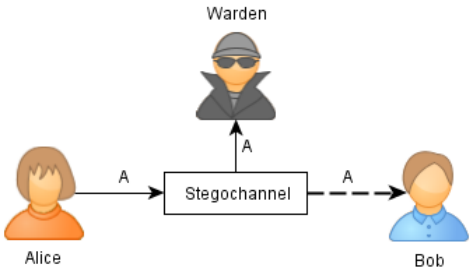

Figure 2: Hidden communication example.

The process of embedding is explained by the Figure 3 where C denotes the cover image and C' the stego-image. Let K represent an optional key (a seed used to encrypt the message or to generate a pseudorandom noise which can be set to {ϕ} for simplicity) and let M be the message we want to communicate. Em is an acronym for embedding and Ex for Extraction.

$$Em: C \times K \times M \rightarrow C' \qquad (1)$$

$$\therefore Ex(Em(c, k, m)) \approx m, \qquad \forall\, c \in C, k \in K, m \in M$$

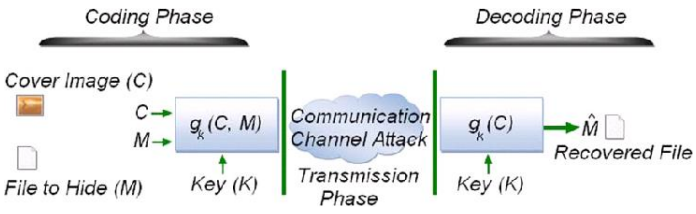

Figure 3: View of the basic mechanism of data hiding (Bajpai & Saxena, 2012).

The core concept of digital image steganography is to hide the secret message in the pixels of the image. Each pixel is basically composed of three color components, Red, Blue and Green, each consisting of one byte. The ASCII values of the text messages are over written in the bits of these pixels. But by doing this, original image is distorted and intruder may easily guess that something is hidden here. So, in most of the cases, least significant bits of the pixels are used for hiding the text.
In this paper, before the embedding the secret message (transcript) has to be encrypted using RSA algorithm to enhance the secrecy of the message. Embedding secret message (transcript) is in the Least Significant Bit (LSB) of each RGB pixels value of the cover image.

2 Review of Related Works

Brahmateja *et al.* (2012), presented a technique to hide data in the edges of the image by extending the Least Significant Bit embedding algorithm. This algorithm hides data in the edge pixels and thus ensures better security against attackers. The proposed algorithm ELSB hides data in edge pixel and is applicable to all kinds of images and can also be used in covert communication, hiding secret information like copyrights, trade secrets and chemical formulae. The algorithm can be used in image steganography but will be more secured when combine with cryptography.

Shrestha and Timalsina (2014), in this research, steganography technique using Daubechies Discrete Wavelet Transform (DWT) is used to embed the secret information and different test are performed. The diagonal band of wavelet transform carries less information of original image and hence coefficients of this band can be used to embed the secret information without much change to an original image. Instead of taking single band, embedding secret information in combination of bands gives better result in terms of Mean Square Error (MSE). The tests did not cover colour image while some documents can be in colour and better embedding algorithm can be used to improve performance.

Sensarma and Sarma (2015), in this paper, a new steganography technique has been proposed using Graphical codes and also comparison with steganography technique using BCH codes has been studied. Using Graphical Code gives better embedding efficiency than using BCH code. Comparison was not done with other steganography techniques and need to improve the security of the techniques by using cryptography secret key or public key.

Abboud (2015), in this research, it shows how to protect several digital documents by using visual cryptography and the Least Significant Bit (LSB) steganography method. LSB is data hiding methodology used to protect secret data from unauthorized access by embedding bits of secret data (such as digital document image) inside the least significant bits of preselected cover image. The first method provides acceptable security with good document image quality. However, the second method provides strong security with some degradation in the document image quality after extraction. Visual cryptography and steganography was used to protect multiple digitized documents from threats created by unauthorized people and the methods protect multiple digital documents simultaneously. Biometric, watermarks and other cryptography algorithm can be used so that there will be comprehensive security methods which will include integrity, authentication and confidentiality.

Halder *et al.* (2016), in this paper, the technique uses a hash function to generate a pattern for hiding data bits into LSB of RGB pixel values of the cover image. This technique makes sure that the message has been encrypted before hiding it into a cover image. If in any case the cipher text

got revealed from the cover image, the intermediate person other than receiver cannot access the message as it is in encrypted form. Embedding the secret message in the LSB of each RGB pixels value of the cover image, before embedding the secret message have to be converted to cipher text using RSA algorithm to enhance the secrecy of the message. In this approach, implementing Hash-LSB derived from LSB insertion on images. In this Hash-LSB, using a hash function to evaluate the positions where to hide the data bits or to be embedded it. Combine the two technologies, one of them is RSA algorithm from cryptography and other is Hash-LSB from steganography was a challenging process. The approach implemented is more secure and more efficient in that the cryptographic method i.e. RSA algorithm to secure the secret message so that it is not easy to break the encryption without the key, while the steganography embedding technique uses hash function and also provide encryption of data uses RSA algorithm; makes our technique a very much usable and trustworthy to send information over any unsecure channel or internet. The implementing enhanced steganography that can have the authentication module along with encryption and decryption can be done to make it more secured.

3 Methodology

This paper proposed a solution for transferring academic transcript without any compromise in security over an in secure channel. In our proposed system, we select a true colour image of size 512 x 512 as a cover image and a secret message (transcript) which is embedded in the true colour image. The secret message (transcript) is encrypted using RSA algorithm, the encrypted (secret message - transcript) is embedded in the Least Significant Bit (LSB) of each Red, Green and Blue (RGB) pixel value of the cover image.

3.1 System Requirement

In order to develop a steganographic system, a requirements specification is necessary. This way the client could define the goals that need to be achieved and the requirements that the developers need to consider during development. The requirements specification should contain functional and non-functional requirements, where functional requirements define the services the system should provide and non-functional requirements are constraints on those services. The authors suggest a systematic approach to develop requirements specification for steganographic systems: it starts with the definition of goals of the future system and ends with the selection of the possible algorithms.

3.2 System Design

The system design of the new system put various variables into consideration like the input specification and design, output specification and files design etc. This section discusses the variables that make up the new system. Steganography system requires any type of image file and the information or message that is to be hidden. It has cryptographic and steganographic modules.

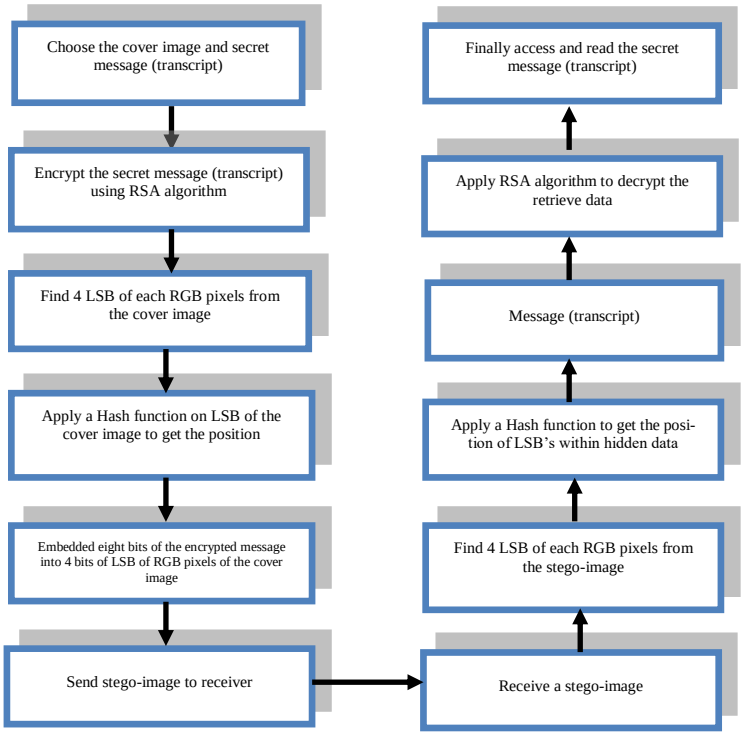

Figure 4: Flow Chart of the New System Model

3.2.1 RSA Encryption Algorithm

The following procedure describes how to select the public key (*Pub*) and the private key (*Priv*) in the RSA algorithm:

i. Select at random two large prime numbers, *p , q*.
ii. Make *n*, the modulo, equal to $n = p.q$.
iii. Calculate Euler's function, $j(n) = j(p.q) = (p - 1)(q - 1)$.
iv. Select a number *Pub*, and test to verify that is relatively prime to j (*n*) by using Euclid's algorithm.
v. Find *Priv* so that it satisfies Equation 5-10, $Pub.Priv = 1 \bmod j(n)$, by calculating the multiplicative inverse of *Pub* using Euclid's algorithm. The properties of j (*n*) guarantee that if *Pub* is relatively prime to j *(n)*, then there is always a multiplicative inverse, which in our case is *Priv*.
vi. Make *n* and *Pub* public; keep j (*n*) and *Priv* secret.

3.2.2 Text Hiding in Color Image Algorithm

i. Read the cover medium i.e. color image.
ii. Read the secret data and perform binarization.
iii. Compare size of binarized secret data against size of cover image to ensure that the cover image is not distorted after embedding.
iv. Perform angular transformation to 90 degree of rotation to the cover and select LSB bits of red, green, blue channels of the cover image
v. Starting from the first pixel (top-left), insert the binarized text in the RGB components of the pixel in 3-3-2 allocation i.e. 3 LSBs of red component, 3 LSBs of green component and 2 LSBs of blue component.
vi. The number of pixels utilized in embedding the text i.e. number of bits inserted, is written in LSB of the last pixel of the image.
vii. Perform reverse angular transformation to retain original position of the cover.
viii. Output is the stego image

3.2.3 Secret Data Retrieval Algorithm

i. Read the stego image and perform angular transformation of 90 degree.
ii. Starting form the first pixel position, extract binarised data from the red, green and blue components of pixel, using 3-3-2 rule, from stego image until the last text bit embedded is extracted. The size of the embedded text is written in the last pixel of the stego image.
iii. Reconstruct the secret message from the extracted bits.
iv. Output is the secret message (transcript).

3.3 System Implementation

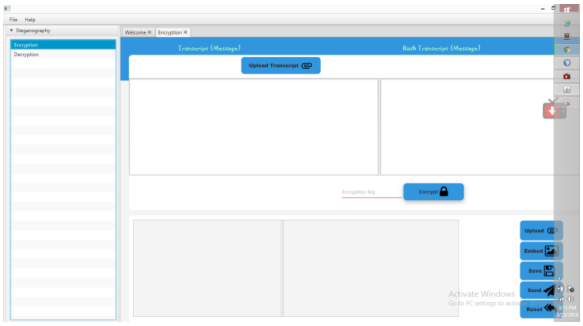

Figure 5: Choose the cover image and secret message (transcript)

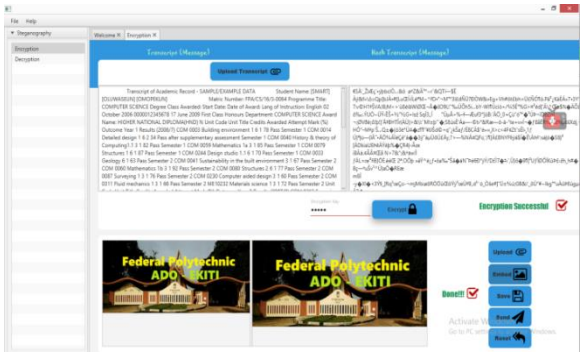

Figure 6: Encrypt the secret message (transcript) using RSA algorithm

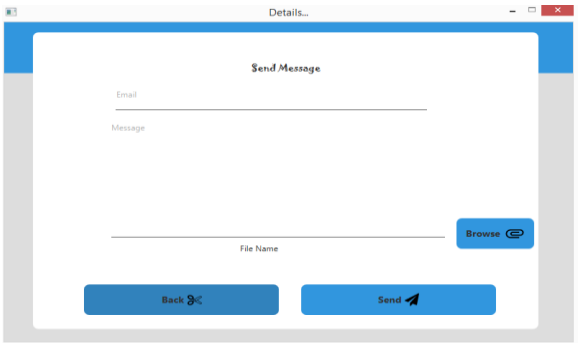

Figure 7: Send stego-image to receiver

Figure 8: Access and read the secret message (transcript)

4 Conclusion

Protecting data from unauthorized access is major concern in the today's fast communication world. A new way of hiding information in an image with less variation in image bits has been discussed in this paper. This technique also applies a cryptographic method i.e. RSA algorithm to secure the secret message so that it is not easy to break the encryption without the key. As contribution, the work presents non-conventional means for providing digital documents protection to support the certificate and transcript administrative work by means of steganography techniques. A secured Hash based LSB technique for image steganography has been implemented. An efficient steganographic method for embedding secret messages into cover images without producing any major changes has been accomplished through Hash-LSB method.

References

Abboud, A. J. (2015). Protecting Documents Using Visual Cryptography, *3*(2), 464–470.
Bajpai, S. and Saxena, K. (2012). Techniques of Steganography for Securing Information : A Survey, *3*(1), 48–54.
Brahmateja, K. N., Madhumati, G. L. and Rao, K. R. K. (2012). Data Hiding Using EDGE Based Steganography, *2*(11), 285–290.
Fischer, Igor and Thorsten Herfet (2007). Watermarks and Text Transformations in Visual Document Authentication, Journal of Computers, 2(5), 44 - 53
Fischer, I and Herfet T. (2006). Visual CAPTCHAs for Document Authentication. Proceedings of the IEEE International Workshop on Multimedia Signal Processing (MMSP), IEEE, 471 - 474
Halder, R., Sengupta, S., Ghosh, S. and Kundu, D. (2016). A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique *18*(1), 39–43. https://doi.org/10.9790/0661-18143943
Sensarma, D. and Sarma, S. Sen. (2015). Data Hiding using Graphical Code based Steganography Technique, *27*(3), 143–147.
Shrestha, A. and Timalsina, A. K. (2014.). Image Steganography Technique Using Daubechies Discrete Wavalet Transform, proceedings of IOE Graduate Conference, 94–102.
Singh, K. U. (2017). Video Steganography Techniques : A Survey, (May), 687–695.
Trivedi, H. and Rana, P. A. (2017). A Study Paper on Video Based Steganography, *3*, 612–615.