IAIC Transactions on Sustainable Digital Innovation (ITSDI)
Vol. 1 No. 1 October 2019

Transaction Document Security Protection In The Form Of Image File, Jpg Or Tif Interbank Transfer Using Steganography And Cryptography

Sucipto Basuki[1], Reksa Anugrah[2]
Sekolah Tinggi Manajemen Informatika dan Komputer Insan Pembangunan
Jl. Raya Serang Km. 10 Bitung – Tangerang. Tlp.(021) 59492836, Fax. (021) 59492837
Indonesia
e-mail: ciptainsan@yahoo.com[1] , reksa_anugrah@yahoo.com[2]

Author Notification
12 October 2019
Final Revised
18 October 2019
Published
21 October 2019

To cite this document:
Basuki, S., & Nugraha, R. (2019). Transaction Document Security Protection In The Form Of Image File, Jpg or Tif Interbank Transfer Using Steganography And Cryptography. IAIC Transactions on Sustainable Digital Innovation, 1(1), 42-48.
Retrieved from https://aptikom-journal.id/index.php/itsdi/article/view/12

Abstract

Information security process can be done by hiding the information on other media or by certain methods, so that other people do not realize there is some information in the media. Technique known as Steganography and Cryptography. Steganography is a technique to hide or disguise the existence of secret messages in the media reservoirs. While Cryptography disguise the meaning of a message, but do not hide that there is a message. In a bank cannot be separated in the presence of inter-bank transactions which transfer if the transfer interbank transactions done in branch offices and nominal transaction exceeds the transaction limit branch offices will require official approval in the upper branch. How do I prove the authenticity of the document transfer transaction? Therefore, a company in the banking sector needs to be a medium to prove the validity of the document sent by the branch transaction. In this case the author has designed an application with a blend of steganography and cryptography techniques that can be used in testing the validity of the transaction document. By using steganographic techniques undercover in a media that has brought and cryptographic key assignment as random, then the document that is sent in the branch office can be proved.

Keywords: Steganography, Cryptography, certificates, validity, proof

1. Introduction

Information exchange through Internet media is one of the advantages gained from the development of today's technology. How to maintain the security of data sent and ensure the validity of the data received is one of the main objectives. In the computer world, there are 2 terms of data security techniques that are very well known namely steganography and cryptography. Steganography is a technique to conceal or disguise the presence of secret messages in their media. While cryptography hides the meaning of a message, it does not conceal that there is a message. In theory, all files in the computer can be used as a message container media, such as JPG, TIF, BMP, audio files formatted as MP3, WAV, even in a video with AVI format, or in other formats such as TXT, HTML, Pdf.

In a banking, there is no interbank transfer transaction. If the interbank transfer transaction is made by a helper whose nominal transaction does not exceed the limit of the branch office transactions will not be a constraint because it does not require approval of officials above the branch office. Another story if the transaction at the branch office was nominative exceed the transaction limit of the branch, meaning that inter-bank transfer transaction requires approval of officials above the branch office. The Office of the branch is downloading the inter-bank transfer document through an office email. What would be the proof of the authenticity of the document transaction sent from the branch office? Therefore, a banking needs to have media to prove about the validity of the documents sent by the Assistant branch office. With a steganography technique that performs disguises on the media below and cryptography that has a task as a random key, the document sent by the branch office can be prove.

1.1 Purpose

The purpose of this research is to design a system or application using steganography and cryptographic techniques used for encryption and test the validity of digital data, especially document banking transactions in the form of JPEG files, BMP and TIF. The officer will mengapprove the transaction will feel secure.

1.2 Problem Limits

The problems found during the study were limited by the following, the implementation of steganography technique to secure Digital document transaction data in the form of JPEG, BMP and TIF files and cryptographic techniques to identify the contents of the message From digital data document with decrypt method.

2. Literature

In the computer world, there are 2 terms of data security techniques that are very well known namely steganography and cryptography.

2.1 steganography

According to Jati Sasongko from the Faculty of Information Technology, Stikubank University Semarang. The year 2004 titled "Securing Information Data using Classical cryptography", steganography is the science and art of hiding hiding messages in such a way that the existence of the message is not detected by Human senses. The word "steganography " comes from the Greek "Steganos", meaning "hidden or veiled", and "Graphein", "wrote".

A steganography (plaintext) message, encrypted with some traditional meaning, produces a ciphertext. Then, the Covertext is modified in some way so it contains a ciphertext, which generates a stegotext. For example, font size, space size, typeface, or other covertext characteristics can be manipulated to carry hidden messages. Only the receiver (who must know the technique used) can open the message and decrypt it. The Format commonly used using steganography techniques include:

- Image Format: Bitmap (BMP), TIF, PCX, JPEG, etc.
- Audio formats: WAV, VOC, MP3, etc.
- Other formats: text files, HTML, PDF, etc.

2.2 Cryptography

Cryptography (cryptography) is the science and art to keep messages safe. (Cryptography is the art and science of keeping messages secure) "Crypto" means "secret" and "graphy" means "writing". The perpetrator or a cryptographic practitioner is called cryptographers. A cryptographic algorithm (cryptographic algorithm), called Cipher, is a mathematical equation used for the encryption and decryption process. Usually both mathematical equations (for encryption and decryption) have a mathematical relationship that is quite close. Encryption is used to encode data or information so that it cannot be read by unauthorized persons. Encrypted Data can be encoded by using a key. To open (decrypt) The data is also used as a key with the key to encrypt (for the case of private key cryptography) or with a different key (for the case of public key cryptography).

2.3 Steganography And Cryptography Differences

Steganography and cryptography have different working principles, although both have close ties in the world of data security.

The result of cryptography is usually a different data from the original form and usually data as if it is a mess so it cannot be known what information contained therein (but can actually be restored to the original form through the process And the output of steganography has the same form of perception as the original shape. The similarity of such perception is by the human senses (especially visual), but when used computers or other digital processing devices can be clearly differentiated between before the process and after the process.

3. Research Method

3.1 Analysis phase

Literary studies, this study was conducted by searching and studying several literature and articles on steganography and cryptography as a reference in the planning and manufacturing of systems or applications.

Defining and analyzing problems to find the right solution

Library Study

3.2 Phase of Program Creation

The design and implementation of the system is done in an ecperimental, which is experimenting to create programs based on the materials and algorithms that have been studied.

3.3 Testing Program

The testing was instituted against the program that was created.

3.4 Literature Review

With many applications or tools graphic design software and photo editing circulating on the market it is very vulnerable to the document in Palsukan. And how to form a banking response to ensure customer transactions are safe. If the case is an inter-bank transaction done in the nominal branch does not exceed the limit of the branch office there is no problem because it does not require approval of branch offices above the branch. What if the case is an inter-bank transaction with the limit exceeded that branch office, requiring approval of officials over the branch office? How can the interbank document transaction be checked for its origin? Based on the case it is necessary to draft a system that can perform the function, so that the authenticity of document transfer transaction between banks can be held accountable. The following is presented illustration of problems experienced in inter-bank transfer transactions that are nominative exceeds the limit of branch offices and require approval of officials above the branch office.

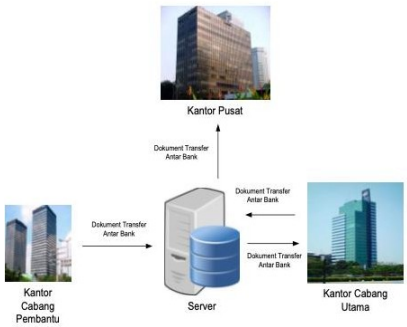

Figure 1. Inter-Bank Transfer transaction illustration that requires Approval office in branch

To answer the problem we need to study the existing problems of previous research so that the final result can solve the problem. This study was conducted by searching and studying several literature and articles on steganography and cryptography as a reference in the planning and manufacturing of systems or applications. In the effort to develop this research should be conducted as one of the implementation of research methods to be conducted. Among them

are identifying the similarities of steganography and cryptography, identifying the methods that have been done, continuing previous research, and knowing others whose specializations and research areas are the same in This. Some of the Literature reviews are as follows:

1. The research was done by Jati Sasongko from the Faculty of Information Technology, Stikubank University Semarang. The year 2004 is titled "Securing Information Data Using Classic cryptography". This study discusses the algorithm used to determine the power of encryption. The security of an algorithm used in encryption or decryption depends on several aspects. One aspect that is quite important is the nature of the algorithm used. When the power of an algorithm is highly dependent on the knowledge (know or not) of the algorithm used, the algorithm is called "Restricted algorithm". If the algorithm is leaked or caught by the crowd, the messages may be legible. Of course, this still depends on the presence of good cryptographers. If no one knows, then the system can be considered safe (albeit false) [1].
2. The research was conducted by Yogie Aditya, Andhika Pratama and Alfian Nurlifa of the Faculty of Industrial Technology, Universitas Islam Indonesia in 2010 titled "Literature Study for Steganography with several methods". The research is done using the method LSB (Least Significant Bit) and EOF (End Of File). In this study, it was explained that the LSB method works by adding bits of data to be hidden (messages) in the last bit most suitable or less meaningful. So if viewed based on the size of LSB Stego image is better because it does not resize the file is being simulated, but for image quality, LSB reduces the quality of the original image. The way EOF method works is to add data or files that will be hidden more than the image file size. The hidden Data will be inserted at the end of the file so that the image file will look slightly different from the original. There are special markers visible from the image file at the very bottom such as stripes. So for image quality, EOF is better because the image quality is maintained, but the file size is larger than before being simulated by the message [2].

No	Metode	Size Image	Size Pesan	Stego Image
1	LSB	150x200	422 karakter	150x200
2	EOF	150x200	422 karakter	153x200

Table 1. Table results comparison Stego Image size

3. This research was conducted by David, A. Murtado and Utin Kasma of Informatics Engineering Study Program, Informatics Management College and Pontianak computer year 2012 titled "Steganography Image with Least Significant Bit method for protection Communication on Online Media ". This study discusses steganography applications with the LSB method that overcomes the insertion of various types of data with different extensions. The size of the bitmap file after being brushed (Stego Bitmap) does not experience a change from the previous bitmap file size (the Cover Bitmap). The LSB method can also manipulate BPC (Bit Per Channel) to enhance the tamping of the bitmap cover to the fullest extent possible. With the LSB method, the efficiency of encryption time and decryption are fast relatife and data integrity before and after the extract process does not undergo any changes at all. [3]
4. This research was done by Andreas Westfeld. Technische Universit¨at Dresden Institute for System Architecture, Germany in 2006 titled "Steganalysis in the Presence of Weak Cryptography and Encoding" the study addressed issues in Weaknesses in cryptography on ecoding. [4]

From the Literature review which expressed above we can draw a bright spot to solve the problems we are facing with steganography and cryptography techniques. Both of these techniques can be applied to a document inter-bank transfer transaction that is sent branches of that type of need and in combining with steganography and cryptography feeding the concept

that occurs is for important documents Then simply perform steganography as a proof of the authenticity of a document in the branches. Whereas if the document is very confidential then for steganography and cryptography collaborate. For more details about the above problems eating explanation can be described as follows:

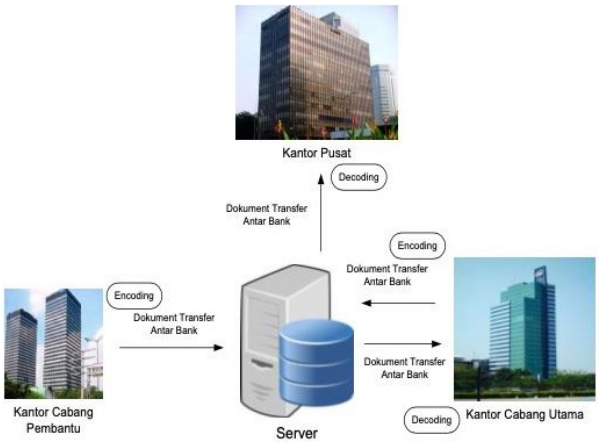

Figure 2. Inter-Bank Transfer transaction illustration that requires Approval office in branch

4. Findings

4.1 Algorithm

After the stage of the mindset and the plot of the concept is already obtained then here will show the algorithm of the application that corresponds to the above draft. Here is a flowchat image during the message insertion process.

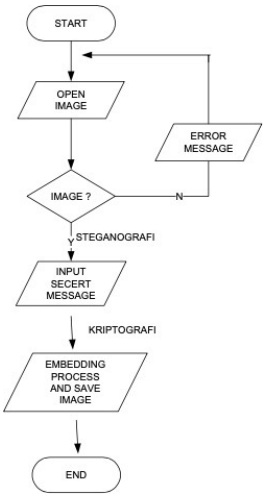

Figure 3. Embedding flowchart

Here is a flowchart image to return the inserted text message, resulting in a text message from the image.

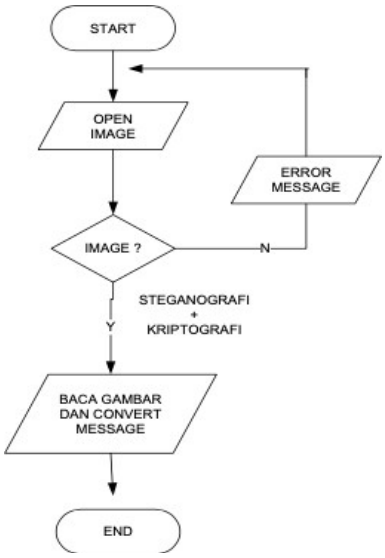

Figure 4. Extraction Flowcharts

4.2 Finding Result

Gambar 5. Tampilan Program

4.3 Analysis

From the Figure 3 flowchart, the program flow can be explained that the program will perform validation of the uploaded image. The requirement is that the file must be an image or JPEG, TIF or BMP. If the user wants to create a Stegano file to insert a message, then simply fill in the message to be inserted in the provided text box and the system will encrypt the data. Save Image button will save the result of the file we have inserted the message.

From the Figure 4 flowchart, you can explain the flow of the program to open the inserted message or text in the image we've done the Stegano process. The process is almost the same as the embedding process, which is open image image that will be opened message content. Then click the Get Information button to convert the message and decrypt data.

4. Conclusion

From the results of the experiment system that has been made, it can be concluded that the file is experiencing the embedding process or the message insertion process, the file does not undergo many changes in other words the resulting image is still the same as the original file, only Different in size or size.

By using steganography and cryptographic techniques it allows for the validity validation of a transaction document transmitted by the Branch

References

[1] Aditya, Y., Pratama, A., & Nurlifa, A. (2010). Studi pustaka untuk steganografi dengan beberapa metode. *Jurnal Fakultas Hukum UII*.
[2] Utomo, T. P. (2012). Steganografi Gambar dengan Metode Least Significant Bit untuk proteksi komunikasi pada media online (Doctoral dissertation, UIN Sunan Gunung Djati Bandung).
[3] Sasongko, J. (2005). Pengamanan Data Informasi menggunakan Kriptografi Klasik. *Dinamik*, *10*(3).
[4] Utami, E. (2009). Pendekatan Metode Least Bit Modification Untuk Merancang Aplikasi Steganography Pada File Audio Digital Tidak Terkompresi. *Jurnal Dasi*, *10*(1).
[5] Westfeld, A. (2006, November). Steganalysis in the presence of weak cryptography and encoding. In *International Workshop on Digital Watermarking* (pp. 19-34). Springer, Berlin, Heidelberg.