http://ejournal.seaninstitute.or.id/index.php/InfoSains
Jurnal Info Sains : Informatikan dan Sains, Volume 11, No 01 Maret 2021
E-ISSN.2797-7889, P-ISSN.2089-3329

Semi-public watermarking digital implementation in the concealment of text messages

[1]Noferianto Sitompul, [2]Maranata Pasaribu
[1]Multimedia Engineering Study Program, Politeknik Negeri Sambas,Kalimantan Barat,
[2]Informatics Engineering Study Program, Akademi Manajemen Informatika dan Komputer Medan Business Polytechnic (MBP) Medan
Email : noferianto88@gmail.com[1], maranata19@gmail.com[2]

Keywords

Digital
Semi-public
Watermarking
Cover message
Step message
Watermarking

Abstract. The purpose of this study is to generate watermarking of an input image. The watermarking process will begin with the process of reading color image pixels. After that, the process will be continued by calculating the step message value inserted and inserting all the necessary values in the watermarking checking process. In the event of an attack, then at the time of watermarking formation, a specific noise value (randomly generated) will be calculated to be inserted into the image. After the process of watermarking formation, then the process can be continued with checking watermarking and extracting messages.

1. INTRODUCTION

Information hiding (IH) is a new area of information security. The goal of the IH design is to hide the message even though, in reality, in the statement, there may be useless data (usually referred to as a cover message / CM). Watermarking (WM) is one of IH's applications. CM should be combined with some other information, such as the identification of the owner. Then the identification code is permanently affixed to the data and must remain available between the data after any transformation process performed by the attacker performed to remove the WM, maintaining the quality of the CM.

One solution developed for digital imagery is to use digital watermarking. Watermarking works by inserting information that leads to ownership, purpose, or other data in digital imagery called watermarking. Watermark insertion is done to not damage the protected digital image and can not be felt by the human senses. Watermarking is a steganography technique to hide information on a media without any significant changes to the press). watermarking scheme inserts digital information called watermark into digital data called carrier. The watermark that can be inserted in the form of plain text, audio, imagery, or video depends on the capabilities of the media it is riding. The addition of a watermark to a multimedia material without affecting its quality can be used as evidence of authentic data ownership. For the security of confidential information, one of the ways the information will be encrypted first before it is inserted into the digital media. Steganography is a technique of hiding personal data into other data media so that confidential data is not known or realized by others.

2. METHOD

2.1. Research Steps

Support this Research Activity by following the following working steps:

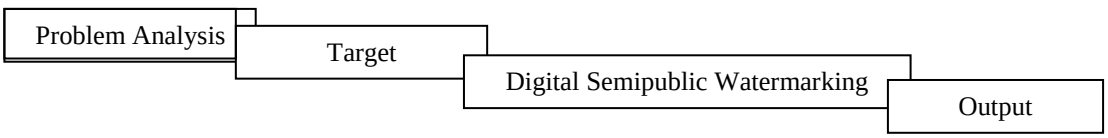

Figure 1. Research Methods

At the stage of the problem, analysis is an activity to ascertain the issue against the concealment of text messages. The process of determining targets with activities for the determination of the intended text target is continued with the application of Digital Semipublic Watermarking.

2.2. Watermarking

There are several definitions of watermarking; among others watermarking means a concept to insert a data or pattern into a document[1]. A piece of information such as ownership or identity of consumers entitled to use it is in the data. In addition, Watermarking is a form of Steganography (Science that learns how to hide data on other data), in learning techniques how to store digital data into another digital host data (The term host is used for data / digital signals that are boarded.)[2]. However, there is a difference between watermarking and steganography. Suppose in steganography confidential information is hidden in digital media where the container media does not mean anything, then on watermarking. In that case, it is precisely the digital media that will be protected ownership by providing certain information in it. Watermarking is somewhat different from watermarks on banknotes. Watermarks on banknotes can still be seen by the naked human eye (perhaps in certain paper positions), but watermarking on digital media here is intended not to be felt by humans without the tools of digital processing machines such as computers and the like[3]. Watermarking takes advantage of the flaws of the human sensory system, such as the eyes and ears. With this deficiency, this watermarking method can be applied to various digital media. So watermarking is a way to conceal or embed certain data /information (either only in public or confidential records) into another digital data. Still, it is not known its presence by the human senses(sense of vision or purpose of hearing) and can face processing digital signals to some degree.

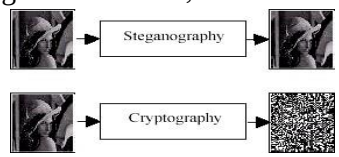

Figure 2. Illustration of Steganography and Cryptography in Imagery

2.3. Digital Watermarking

Digital watermarking is the insertion of digital signals into digital media. Digital watermarking departs from processing digital signals, where digital signals can be in the form of images, audio, video, and text[4]. As mentioned earlier, that digital watermarking is implemented by utilizing the shortcomings of the human senses (senses of vision and purpose of hearing) where the human reasons are less sensitive to changes that occur, such as changes that appear at the bit level (to some extent), changes in frequency levels (beyond the frequencies received by humans)[5]. The idea of watermarking digital data (so-called digital watermarking) was developed in Japan in 1990 and Switzerland in 1993. Digital watermarking is growing as the internet expands; digital objects such as video, imagery, and sound can be easily duplicated and disseminated[6], [7]. The thing that separates watermarking from steganography is that in its implementation, steganography is used to secure information superimposed on digital media while watermarking can be used for a variety of purposes[8].

2.4. Digital Semipublic Watermarking

In the case of step message (SM) or in other words watermarked messages have the form of equations (2.1) below: S(n) = C(n) + w(n), n = 1, 2, …, N …… (2.1) where C(n) is a cover message (CM), w(n) = Δ(n)e(n), Δ(n) is a series of non-negative real values, e(n) is a row of + 1, - 1 and N are the number of WM elements such as CM image pixels[9]. On the first semi- public from WM, deretan e(n) is assumed to be known to each user and is a public key, while deratan (n) is stored in $\eta_w = \frac{\text{var}\,(C(n))}{\text{var}\,(\Delta(n)e(n))} = \frac{3\sigma_C^2}{D^2}$) row uses a free, regularly distributed sample of the one, and (n) also takes a nonnegative sample that is free and distributed regularly at an interval (0, D), where D > 0 is a

fixed positive value. Cover message C(n) is described as a random zero-mean discrete process with a variance of $\sigma\Delta\pm\Delta^2$ The distortion limit after watermarking is given as a signal-to-noise ratio that can be described as seen in the following equation (2.2)[10]:…… (2.2)

Valery Korzhik, Guillermo Morales-Luna, Dmitry Markov, and Irina Markova also introduced for each regular user to detect WM can use the following formula (2.3):

$$\Lambda = \sum_{n=1}^{N} S(n)e(n)$$ ……………………………… (2.3)

If, then a WM has been detected; otherwise, then WM is not detected. If WM is contained in SM, the following formula (2.4) is obtained:$\Lambda \geq \lambda$

$$\Lambda = \sum_{n=1}^{N} (C(n) + \Delta(n)e(n))\, e(n) =: \Lambda_1$$ …………………… (2.4)

If it is not contained in BC, the following formula (2.5) is obtained:

$$\Lambda = \sum_{n=1}^{N} C(n)e(n) =: \Lambda_0$$ …………………………… (2.5)

$$\Lambda' = \sum_{n=1}^{N} S'(n)e(n)$$ ……………… (2.6)

$$\epsilon(n) = \begin{cases} \sigma e(n) & \text{if WM is absent} \\ 0 & \text{otherwise} \end{cases}$$ … (2.7)

Therefore, for an ordinary user who tries to detect WM after an attack, there are two possible results, as seen in the following formula (2.8):

$$E(\Lambda') = \begin{cases} E(\Lambda'_0) = N \cdot \sigma & \text{if WM is absent} \\ E(\Lambda'_1) = \dfrac{N \cdot D}{2} & \text{otherwise} \end{cases}$$ ….. (2.8)

Based on the results of tests conducted by the algorithm developers, it is known that the above algorithms cannot be applied practically, and they recommend applying another semi-public WM method that is based on periodic series, as seen in the following details.
Assume SM is defined as seen in the following formula (2.9): S(n) = C(n) + w(n), where n = 1, 2, ..., $2N_0$………… (2.9) Where: w(n) = (n) …………………………… (2.10) $N\alpha\pi_0 = {}^{N}/_{2}$ ……………………… (2.11) A row (n) is a random row consisting of a 1, periodic, two-period period with a length of $N\pi\pm_0$each. Threshold values can be calculated by using the following formula (2.12):

$$\Lambda = \sum_{n=1}^{N_0} S(n)S(n + N_0)$$ … (2.12)

Meanwhile, to add noise, the following formulas (2.13) and (2.14) can be used:

1. For cases of no WM:

$$\epsilon(n) = \begin{cases} \sigma\tilde{\pi}(n) & , \quad n \leq N_0 \\ \sigma\tilde{\pi}(n - N_0) & , \quad N_0 + 1 \leq n \leq 2N_0 \end{cases}$$ … (2.13)

2. For the case, there is WM:

$$\epsilon(n) = \begin{cases} \sigma\tilde{\pi}(n) & , \quad n \leq N_0 \\ -\sigma\tilde{\pi}(n - N_0) & , \quad N_0 + 1 \leq n \leq 2N_0 \end{cases}$$ …… (2.14)

3. ANALYSIS AND DISCUSSION

To better understand the working process of the Digital Semipublic Watermarking method discussed, the following is given a simple calculation example:

Message: TES Public
key: 15 Private key: - -
+ - - -
Watermarking calculation process:
1. Convert messages to ASCII Code form

1st Character: T=84=01010100
Character ke-2: E = 69 =
01000101 3rd Character:
S=83=01010011
2. Specify the bit length of each cover message subblock

-
Bit length = 5
3. Break cover messages into subblocks

with a length of 5 bits

C(1) = 01010 = 10
C(2) = 10001 = 17
C(3) = 00010 = 2
C(4) = 10101 = 21
C(5) = 00110 = 6

4. Specify the value N0

N0 = 6/ 2 = 3

5. Calculate the value of the step message

-- S(1) = C(1) + W
S(1) = 10 + -15
S(1) = -5 + 255 = 250

S(2) = C(2) + W
S(2) = 17 + -15
S(2) = 2

S(3) = C(3)+ W
S(3) = 2 + 15
S(3) = 17

S(4) = C(4) + W
S(4) = 21 + -15
S(4) = 6

S(5) = C(5) + W
S(5) = 6 + -15
S(5) = -9 + 255 = 246

S(6) = C(6) + W
S(6) = 0 + 15
S(6) = 15

6. Calculate threshold value

Threshold = 250 * 6 + 2 * 246 + 17 * 15
Threshold = 2247

Pasted data: Threshold value and step message (SM) value set S(1) ... S(6). The insertion process is as follows:

Data to insert:
2247, 250, 2, 17, 6, 246, 15

1000 1100 0111, 1111 1010, 0000 0010, 0001 0001, 0000 0110, 1111 0110, 0000 1111

Because the input bit length = 60 bits, the image size must be at least 60 pixels, for example, an input image with a size of 5 x 12 has the following pixel color:

Table 1 : Pixel Bit

125	185	126	178	165	254	211	216	113	65	87	64
125	185	126	178	165	254	211	216	113	65	87	64
125	185	126	178	165	254	211	216	113	65	87	64
125	185	126	178	165	254	211	216	113	65	87	64
125	185	126	178	165	254	211	216	113	65	87	64

Then the insertion process is as follows:
125 = 0111 1101
The bit to be inserted is because the LSB bit = 1, then there is no discoloration. 185 = 1011 1001
The bit to be entered is 0; the LSB bit = 1 will be changed to 0. Results obtained: 1011 100**1**→ 1011 100**0** = 184
126 = 0111 1110
The bit to be entered is 0 because the LSB bit = 0, then there is no discoloration. 178 = 1011 0010
The bit to be entered is 0 because the LSB bit = 0, then there is no discoloration. And so on, until all the bits are inserted into the image pixel color. Message extraction process: Calculate threshold value

---
Result = 250 * 6 + 2 * 246 + 17 * 15
Result = 2247
Result >= Threshold --> Watermarking
Detected Value = 250 + 1 * 15
Value = 265 – 255 = 10
Value = 2 + 1 * 15
Value = 17
Value = 17 + -1 * 15
Value = 2
Value = 6 + 1 * 15
Value = 21
Value = 246 + 1 * 15
Value = 261 – 255 = 6
Value = 15 + -1 * 15
Value = 0
C(1) = 10 = 01010
C(2) = 17 = 10001
C(3) = 2 = 00010
C(4) = 21 = 10101
C(5) = 6 = 00110
C(6) = 0 = 00000
Message (bit) = 010101000100010101010011000000
1st Character:
T=01010100=84 Character
ke-2: E = 01000101 = 69 3rd Character: S= 01010011 = 83

4. CONCLUSION

Based on the results of the tests conducted, information obtained that for *.jpg format images, the size of the watermarking image will increase in size while for *.gif and *.bmp format images, the change in the size of the watermarking image will be relatively small. The semi-public watermarking digital algorithm can be used to add watermarks to the image and can detect the picture even though there has been an attack on the watermarking image. The software can be developed by comparing the semi-public watermarking digital algorithms discussed with other similar algorithms

REFERENCE

[1] S. R. Febriani, "Implementasi Digital Watermarking pada Citra Menggunakan Metode Least Significant Bit," vol. 21, no. 3, pp. 8–18, 2016.

[2] E. Y. Reva, B. Susilo, and E. P. Purwandari, "Aplikasi Watermark Pada Citra Digital Menggunakan Kombinasi Metode Discrete Cosine Transform , Discrete Wavelet Transform Dan Singular Value Decomposition," *J. Rekursif*, vol. 4, no. 2, pp. 152–160, 2016, [Online]. Available: ejournal.unib.ac.id.

[3] K. Firdausy, I. Hawariyanta, and M. Murinto, "IMPLEMENTASI WATERMARKING UNTUK PENYEMBUNYIAN DATA PADA CITRA DALAM DOMAIN FREKUENSI MENGGUNAKAN DISCRETE COSINE TRANSFORM," *TELKOMNIKA (Telecommunication Comput. Electron. Control.*, 2006, doi: 10.12928/telkomnika.v4i1.1240.

[4] T. N. Turnip, J. Doloksaribu, V. Purba, and I. Saragih, "Pengaruh Kapasitas Dimensi Citra Watermark terhadap Audio Watermarking dengan Perpaduan Metode DWT (Discrete Wavelet Transform) dan SVD (Singular Value Decomposition)," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 6, no. 2, p. 141, 2019, doi: 10.25126/jtiik.2019621269.

[5] Y. HAFIZHANA, I. SAFITRI, L. NOVAMIZANTI, and N. IBRAHIM, "Image Watermarking pada Citra Medis menggunakan Compressive Sensing berbasis Stationary Wavelet Transform," *ELKOMIKA J. Tek. Energi Elektr. Tek. Telekomun. Tek. Elektron.*, vol. 8, no. 1, p. 43, 2020, doi: 10.26760/elkomika.v8i1.43.

[6] A. Abdussalam, E. Hari Rachmawanto, A. S. Noor, D. R. Ignatius Moses Setiadi, and C. Atika Sari, "Optimasi Keamanan Watermarking pada Daubechies Transform Berbasis Arnold Cat Map," *J. Inform. J. Pengemb. IT*, vol. 4, no. 1, pp. 31–37, 2019, doi: 10.30591/jpit.v4i1.911.

[7] H. Nuryadi, "Watermarking Dengan Qrcode Digunakan Untuk Verifikasi Pada Website," *J. Sist. Inf. Univ. Suryadarma*, vol. 4, no. 2, pp. 34–41, 2014, doi: 10.35968/jsi.v4i2.4.

[8] S. Syamsuryadi and I. Aqil, "Watermarking Video Menggunakan Metode Transformasi Wavelet Diskrit," *J. Ilm. Inform. Glob.*, vol. 9, no. 2, pp. 90–94, 2019, doi: 10.36982/jig.v9i2.562.

[9] A. Suheryadi, "Penerapan Digital Watermark Sebagai Validasi Keabsahan Gambar Digital Dengan Skema Blind Watermark," *JTT (Jurnal Teknol. Ter.*, vol. 3, no. 2, pp. 1–6, 2017, doi: 10.31884/jtt.v3i2.54.

[10] J. Rosmiyati and T. M. S. Mulyana, "Watermark Dengan Gabungan Steganografi Dan Visible Watermarking," *J. Algoritm. Log. dan Komputasi*, vol. 1, no. 1, pp. 36–43, 2018, doi: 10.30813/j- alu.v1i1.1109.