Secure Electronic Voting System Based on Image Steganography

Lauretha Rura, Biju Issac and Manas Kumar Haldar
School of Engineering, Computing and Science
Swinburne University of Technology (Sarawak Campus)
Kuching, Malaysia
4196139@students.swinburne.edu.my, bissac@ swinburne.edu.my, mhaldar@swinburne.edu.my

***Abstract* — As information technology evolves over time, the need for a better, faster, more convenient and secure electronic voting is relevant since the traditional election procedures cannot satisfy all of voter's demands. To increase the number of voters and to offer an enhanced procedure in an election, many researchers have been introducing novel and advanced approaches to secure electronic voting systems. This paper proposes a secure electronic voting system that provides enhanced security by implementing cryptography and steganography in Java. As a preliminary investigation, two steganography techniques are considered and their performances are compared for different image file formats.**

Keywords – image steganography; electronic voting; visual cryptography; secret-ballot receipts, threshold decryption

I. INTRODUCTION

Voting has played a major role in the democratic societies. Traditional voting procedure uses paper-based ballot. However, this approach is costly, inconvenient and time consuming for voters. Many people nowadays prefer a more instant way to vote. With the evolution of computer technology, many researchers are proposing secure, reliable and convenient electronic voting systems as a substitute to the traditional voting procedure. It thus helps to encourage each voter to make use of their right to vote. Such systems have to be designed to satisfy the following requirements [1]–[7]:

- Completeness – All valid votes are counted correctly.
- Soundness – The dishonest voter cannot disrupt the voting.
- Privacy – All votes must be secret.
- Unreusability – No voter can vote twice.
- Eligibility – No one who is not allowed to vote can vote.
- Fairness – Nothing must affect the voting. No one can indicate the tally before the votes are counted.
- Verifiability – No one can falsify the result of the voting.
- Robustness – The result reflects all submitted and well-formed ballots correctly, even if some voters and (or) possibly some of the entities running the election cheat.
- Uncoercibility – No voter should be able to convince any other participant of the value of its vote.
- Receipt-freeness – Voters must neither obtain nor be able to construct a receipt proving the content of their vote.
- Mobility – The voter can vote anytime and anywhere through internet.
- Convenience – System must allow voters to cast their votes quickly, in one session and with minimal equipment or special skills.

In the recent years, researchers are more focusing on developing a new technology which can support uncoercibility, receipt-freeness and also universal-verifiability. Many end-to-end verifiable systems (E2E) are proposed and being widely used. In principle, E2E voting system offer assurance to the voters as they cast their vote by distributing a receipt of their vote which can be used for verification purpose from the overall tabulation of the collected votes. Yet on the other hand, this receipt cannot be used as a proof in vote buying or vote coercion although all of the receipts will be posted publicly in a secured append-only Bulletin Board once the voter finished the voting process. Therefore, the E2E system would still protect the voter's privacy.

In order to accomplish the previously stated requirements, many schemes have been implemented and proposed. Those schemes are mostly rooted in one particular field of security - cryptography. In electronic voting mechanism, cryptography is used to protect the data transmitted between the voter and the server to ensure that it would not be leaked to a third party. Cryptography theories are also applied in each process in the system to make sure the authenticity of the voter, the originality of the ballot, casted and collected votes, the reliability of the tallied votes and the privacy throughout the election. There are many cryptography methods that can be applied, such as blind signature scheme, homomorphic encryption, oblivious signature scheme, bit commitment scheme, Schnorr identification scheme, mixed-net schemes, digital signature scheme, secure multi-party computation, cryptographic hash-function, etc. However, in this paper only a few selected schemes would be applied in different voting stages to preserve the main characteristics of an electronic voting system. Those schemes are secret-ballot receipts theory, steganography - a branch of information security technique that has not been commonly used in this field, visual cryptography and threshold decryption cryptosystem.

Both branches of information security are combined together in this paper to ensure the design of a secure electronic voting system by providing a double layer of data protection. Secret-ballot receipts theorem introduced by David Chaum [8] is mainly a combination of cut and choose scheme together with a cryptography technique by Naor and Shamir [9], visual cryptography. There are five different stages in the system design architecture such as – registration stage, authentication stage, voting stage, tallying stage, publishing and verification stage. These schemes would be implemented respectively and secret-ballot receipt scheme is going to be applied in the voting stage together with visual cryptography. Right after the voter casted their votes, steganography would be used throughout the system processes for data communication purpose. In the tallying stage, the threshold decryption cryptosystem will be implemented. The combined method is believed to be sufficient to provide a secure, reliable and convenient voting system. Since the proposed tool is an electronic voting system, it is necessary to assume that the voter would complete the voting process secretly.

In section 2 the cryptographic preliminaries that would be applied are explained, followed by the voting procedure description in section 3. The implementation overview based on the proposed approaches is explained further in section 4, including the experimental results on steganography. The conclusion is in section 5.

II. PRELIMINARY APPROACHES

A. *Visual Cryptography*

This scheme was introduced by Naor and Shamir [9]. In cryptography field, visual cryptography offers less computational performance compare to the other cryptography schemes due to their complex cryptographic algorithms used to protect a secret. It encrypts visual information, for example pictures, text, etc. in a particular way and produces a set of shares as the result. These shares need to be stacked altogether by using a visual cryptography tool to reveal the hidden secret [9]–[11].Visual Cryptography is a method for protecting image-based secrets that has a computation-free decryption process [11].

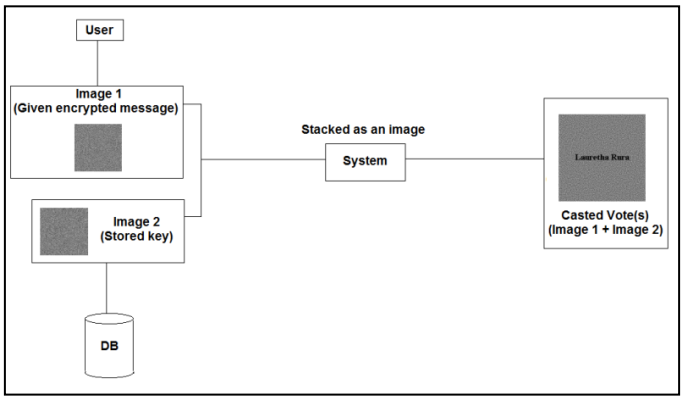

Figure 1. Data flow diagram of how visual cryptography applied in the system

It can be considered as a convenient and reliable tool for secret protection or even for verification (authentication) process because it is not time-consuming, low in computational cost and could still be done without any external devices needed. Illustration on how visual cryptography works in electronic voting system is displayed in Fig. 1.

B. *Image Steganography*

Steganography is the art of hiding information in ways that prevent the detection of hidden messages [12]. It is introduced as a branch of information security based on the needs of providing an enhanced security technique of hiding secret information. As the information technology evolves, more threats arise and a simple encryption method is just not sufficient enough to protect the secrecy of data anymore. An encrypted data could easily cause suspicion since it is clearly shown as one. On the other hand, steganography offers a less suspicious way of hiding a secret. Therefore, steganography is proposed to be used as a main tool in this paper to secure the data communication in the election procedure, as its purpose is to maintain a secret communication between two parties. This scheme could be applied to various types of data such as text, images, audio, video and protocol file format. The methods of steganography vary from invisible inks, microdots, character arrangement, digital signatures, covert channels, to spread-spectrum communications [12]. Unlike cryptography, the input and output data (stego-object) of steganography would be identical. As a result, it would be difficult to recognize and interpret the hidden secret in the stego-object. However some of the steganography schemes like text steganography are limited in data encoding. Thus, they are not completely feasible to be applied in the system. Image steganography on the other hand, give a better encoding technique to be used as it can securely hide the secret message. It supports data transmission process by securely transferring a hidden secret in a digital image file. For this reason, image steganography would be applied in this system together with secret-ballot receipts scheme and visual cryptography in the voting stage and also to be used throughout the system for data transmission process.

Fig. 2 and Fig. 3 shows the comparison of an original and stego-image with very unnoticeable difference. Fig. 2 is the original image and Fig. 3 has been encoded with random encrypted words. Image steganography can be separated into two types based on its compression method, image (spatial) domain and transform (frequency) domain [13]. For image domain, a message would directly be embedded into a source image and then it would be compressed with lossy compression. Therefore, all the embedded information would not be altered in the compression phase. On the other hand, in transform domain, message would be embedded into an image in between the compression phases with both lossy and lossless compression. In general, transform domain is more robust compare to image domain technique because it eliminates the possibility of message being destroyed during the compression process when the excess image data is removed (lossy compression). One of the most used approaches in embedding information in image domain method is Least Significant Bit (LSB). It can be used together with few image file formats, such as BMP and GIF image file. LSB is implemented with a similar characteristic to text

steganography. In text steganography, a message can be hidden in every n^{th} character of a passage, likewise in LSB the secret information would be embedded to the least significant bit (8^{th} bit) or could also be in all of the bytes in an image [13]. LSB is suggested to be used for embedding in a large size image. To encode and decode the hidden secret, a pair of key can be distributed to both sender and receiver as another layer of security. In transform domain technique, JPEG steganography is commonly used in hiding a secret besides Patchwork and Spread Spectrum. It is widely used in the Internet due to the small size of the image after the compression. Patchwork is a method that marks image areas or patches by using redundant pattern encoding to scatter hidden information throughout the cover image [12]. The algorithm adds redundancy to the hidden information and then scatters it throughout the image [13]. As a result, the stego-image would be more resistant to image manipulation, such as rotation or cropping. Similar to patchwork, spread spectrum method hides data by spreading it throughout the cover image without changing its statistical properties [13]. Both methods are suitable to be applied in encoding a small amount of secretive information.

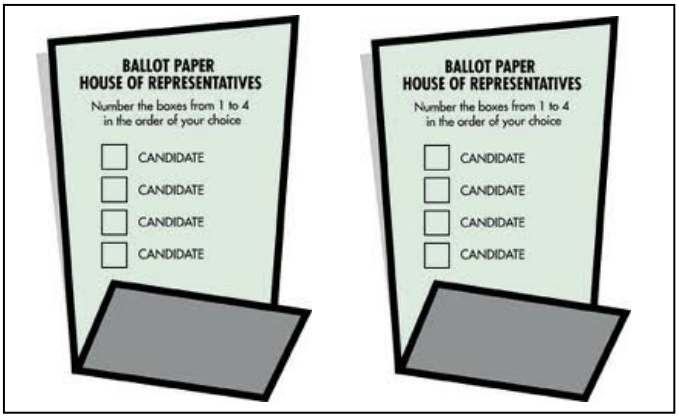

Figure 2. Original Image

Figure 3. Stego-object (original image which has been embedded with a hidden message)

C. *Secret-ballot Receipts*

The principle of secret-ballot receipt lays in the concept where privacy violation should not occur at all in the election, to ensure its integrity and also to prevent altered votes in the election process due to vote buying or selling and vote coercion [8], [14]. The technique provides a direct assurance of each voter's vote. The implementation of secret–ballot receipts scheme helps to reduce the need for physical security, audit and observation in several stages of the system as it does not require any external hardware to be applied as a compliment to its functionality. The initial flow of secret-ballot receipts implementation requires each voter to use an external hardware (printer) in order to retrieve and verify their casted ballots in a printed receipt. It also applies the same concept as Naor and Shamir in visual cryptography [9], where a secret – in this case, a vote that is hidden in two separated layer of pixel symbols. The secret would only be revealed once those layers are overlaying one another. However, to minimize external hardware usage in the election process, instead of generating a printed receipt, the system would then generate a digital receipt in an image format to each voter.

Chaum also proposed the conjunction of mix-net scheme in the secret-ballot receipt to ensure the integrity and privacy of the tallying process [8]. Here, the voter's chosen layer would be passed respectively among few trustees who are going to generate intermediate batches based on voter's receipt batch as an input. The final product of this process is a tally batch in the form of ballot image. However, the processes would be time-consuming because different trustees (servers) are required to be included in the election procedure. Hence, a simple amendment made to the applied mix-net scheme would be introduced in this paper in order to fulfill the system's requirement by implementing threshold decryption scheme.

III. VOTING PROCEDURE

In a paper-based voting procedure, the progress of an election is divided into a few different stages based on each of their role. Likewise in an electronic voting procedure, researchers have implemented and presented their work in a few different stages as well. Described below are the stages where the proposed approaches are to be implemented. In the voting process, it is also assumed that the system contains three main personnel types – election administrator(s), vote tabulation officers and the voters themselves.

A. *Registration Stage*

This stage is also known as the preparation stage. In this phase all of the necessary constraints for the election are prepared. Voter's registration would be carried out to respect the voters' right by ensuring only eligible voters can vote [15]. They would be identified by using their respective organization's email address. As another layer of security during login process, each of them would be prompted to insert few random characters of a secret word that would then be used as authorization key in the next stage.

B. *Authentication Stage*

In a remote electronic voting system, registered voters can authorize themselves by logging into the system. They would be prompted to enter their self-defined username and encrypted password for security purposes. Upon login, the user is required to enter few random characters on their pre-defined authorization key as another layer of authentication. It is proposed as in a remote electronic voting system, stronger protection is required to convince the voters that a proper level of trust has been established between the voter and the system [16]. Once the user has been identified as an eligible voter and successfully logged in to the system, they will see a welcome screen which states their account status and a menu panel where they can navigate to cast their vote.

C. *Voting Stage*

In a paper-based voting, this stage would be carried out by inserting the ballot into a securely sealed box. Similarly in the electronic voting system, this stage is carried out by sending the voter's casted vote in an electronic ballot to the server where all the ballots would be collected and stored. To

minimize the security attack, the sequence of the candidate list could be display randomly by using SecureRandom class from Sun's JCE package. Once the voter submits their vote, it would then be encoded in the ballot by implementing steganography. This ballot will later on be sent over to the tally server as a stego-image. Prior to vote transmission, the vote is going to be 'encrypted' with visual cryptography technique by splitting the vote before it is encoded in an image into few shares. In this system the shares would be limited to two shares. Stand-alone share would not reveal any information to anybody, but once the shares are overlaid (combined) by using a visual cryptography tool, the voter's vote would be revealed. Basically, each voter would be given one layer (share) of the image as their receipt, while the other separated layer of the vote would be kept – or saved by the administrator for the purpose of vote's tally. Therefore, the voters would still be able to verify their votes to themselves and have a better confidence in the system. The data flow during voting submission process in this stage is illustrated in Fig. 4.

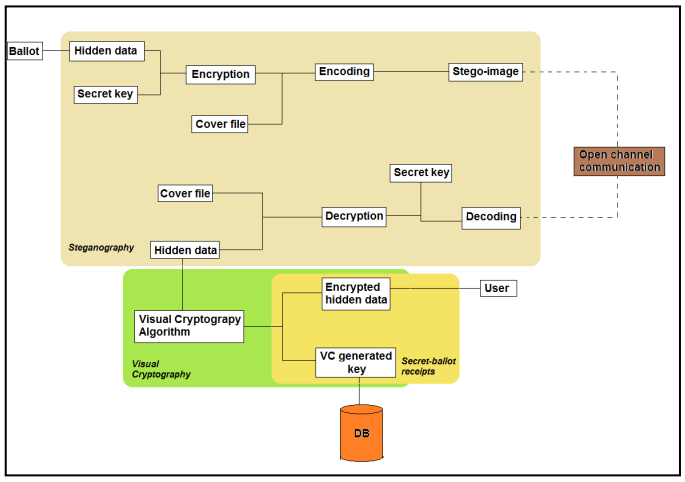

Figure 4. Data flow diagram of voting submission process in Voting Stage

D. *Tallying Stage*

In this stage, all of the collected ballots would be initially 'decrypted' by using the other half of the vote share. In order to perform this decryption process, the private key which has been divided and distributed to a few appointed personnel must be merged together. This method is called the threshold decryption cryptosystem [17] – [19]. Threshold scheme would be implemented in the ballot decryption process to ensure that only the authorized personnel can count the vote. However, all of the votes are stored as cipher texts in the database. Therefore, PKI is going to be applied before votes and can then be retrieved and counted by matching the other half of the shares and the voter's receipt. The votes would then be published for verification purpose.

E. *Publishing and Vote Verification Stage*

In a paper-based voting, once the tally process is done, the authorized personnel will announce the result of the election. However, the voter would not be able to verify their own vote because the authorized personnel will only announce and publish the total result of each candidate. On the other hand, in remote electronic voting system the voters can verify their own votes because each voter receives a share of receipt that would be published in the secured append-only bulletin board. Other than that, the system would also be provided with a vote verification data to check their casted vote. The feature is implemented by combining visual cryptography and secret-ballot receipts together. The process is shown in Fig. 5. In this way, most of electronic voting system's requirements, such as uncoercibility, receipt-freeness, universal-verifiability, etc. would be delivered as neither the user nor the election officials (administrator) has access to identify the collected ballots.

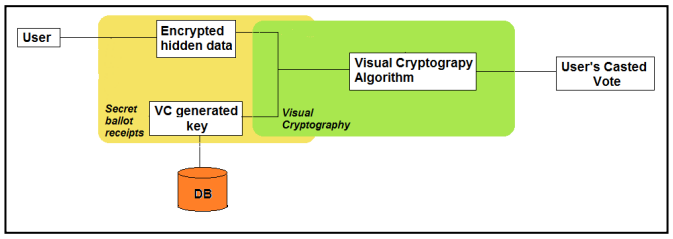

Figure 5. Data flow diagram during verification process in Publishing and Vote Verification Stage

IV. Implementation Overview and Results

A preliminary implementation of steganography on some images is discussed below. As stated before, the compression image steganography has been divided into two categories, such as transform domain that applies lossy compression and image domain which implements lossless compression. For that reason the implementation of image steganography cannot be combined in one single algorithm for both image domain (GIF, PNG, BMP, etc) and transform domain images (JPEG). As a result, in this experiment two different steganography tools, F5 and Outguess are used for image comparison purpose. Both algorithms are explained further in Fig. 6 and Fig. 7 [20].

Input: message, shared secret, cover image
Output: stego-image
initialize PRNG with shared secret
permutate DCT coefficients with PRNG
determine k from image capacity
calculate code word length $n \leftarrow 2k - 1$
while data left to embed **do**
get next k-bit message block
  repeat
  $G \leftarrow \{n$ non-zero AC coefficients$\}$
  $s \leftarrow k$-bit hash f of LSB in G
  $s \leftarrow s \oplus k$-bit message block
    if $s \neq 0$ **then**
      decrement absolute value of DCT coefficient Gs
      insert Gs into stego image
    end if
  until $s = 0$ or $Gs \neq 0$
insert DCT coefficients from Ginto stego image
end while

Figure 6. Transform domain steganography algorithm (F5)

```
Input: message, shared secret, cover image
Output: stego-image
initialize PRNG with shared secret
while data left to embed
    do
    get pseudo-random DCT coefficient from cover image
    If DCT ≠ 0 and DCT ≠1 then
        get next LSB from message
        replace DCT LSB with message LSB
    end if
    insert DCT into stego image
end while
```

Figure 7. Image domain steganography algorithm (Outguess)

The experiments were done for five types of images based on their coloration, such as Grayscale, Colored, also Red, Green and Blue Toned images with 856 bytes text file as a secret message that would be encoded in 24 bit image depth. Each image is represented in three color channels, such as Red, Green and Blue with the length of 8 bits for each channel. The results are shown in more detail in Table 1 and Table 2.

TABLE I. COMPARISON OF AN ORIGINAL IMAGE (JPEG FILE FORMAT) AND A STEGO-IMAGE (TRANSFORM DOMAIN) EMBEDDED WITH A JPEG STEGANOGRAPHY TOOL BASED ON FIVE DIFFERENT IMAGE COLOR TONES

	Greyscale	Colored	Red Toned	Green Toned	Blue Toned
Initial Size	11.3kb	14.2 kb	10.8kb	15.7kb	22.2kb
Stego-image Size	9.5kb	7.4 kb	8.4kb	8.5kb	11.6kb
Initial Number of Image's Colors	5301	18584	13429	16745	37395
Number of Stego-image's Colors	6760	19552	14548	17986	39913
Bit Depth	24	24	24	24	24
Dimensions (Width x Height)	200x150 pixels	200x150 pixels	200x150 pixels	200x150 pixels	300x250 pixels
Initial Image Resolutions	300x300 dpi	72x72 dpi	100x100 dpi	300x300 dpi	600x600 dpi
Stego-image Resolutions	300x300 dpi	300x300 dpi	300x300 dpi	300x300 dpi	300x300 dpi

As shown in Table 1 and Table 2, each of the numbers of the stego-images is larger compare to its original image. This is because by embedding a message, the number of noise and the altered LSB pattern in the original image would be increased. As a result, the stego-image size and its resolutions (for PNG file format) would be enlarged.

Compared with the PNG file format, stego-images in JPEG file format produced a much lesser size image as their end result. However, they have larger amount of colors compared to the stego-images in PNG file format. Another element that could be taken into consideration to compare both image file formats is their histogram level. It can be used as one of the aspects to ensure the security assurance of the system.

TABLE II. COMPARISON OF AN ORIGINAL IMAGE (PNG FILE FORMAT) AND A STEGO-IMAGE (IMAGE DOMAIN) EMBEDDED WITH A LSB STEGANOGRAPHY TOOL BASED ON FIVE DIFFERENT IMAGE COLOR TONES

	Greyscale	Colored	Red Toned	Green Toned	Blue Toned
Initial Size	23.3kb	60.1 kb	54.5kb	54.0kb	63.1kb
Stego-image Size	45.9kb	78.9 kb	65.3kb	88.6kb	76.2kb
Initial Number of Image's Colors	256	23465	13649	26910	23924
Number of Stego-image's Colors	891	23500	14323	27000	23990
Bit Depth	24	24	24	24	24
Dimensions (Width x Height)	200x150 pixels	200x150 pixels	200x150 pixels	200x150 pixels	300x250 pixels
Initial Image Resolutions	180x180 dpi	72x72 dpi	300x300 dpi	300x300 dpi	72x72 dpi
Stego-image Resolutions	300x300 dpi	300x300 dpi	300x300 dpi	300x300 dpi	300x300 dpi

As observed from both original and stego-image histogram of colored images in JPEG and PNG format in Fig. 8, 9, 10 and 11 above, it can be concluded that there are only slight changes in their histogram level after secret message is embedded. Therefore, based on those previously described aspects, image steganography could be applied into this proposed electronic voting system with the implementation of JPEG file format as its cover image and stego-image file format.

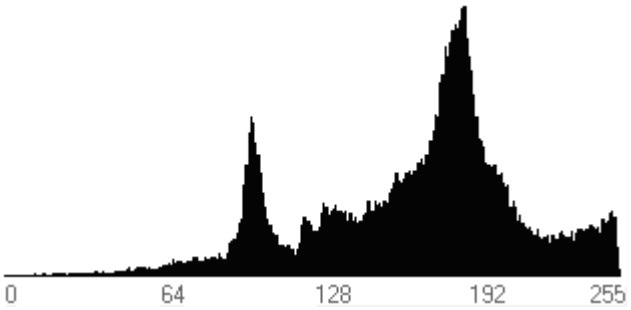

Figure 8. Original image histogram of the colored image (JPEG)

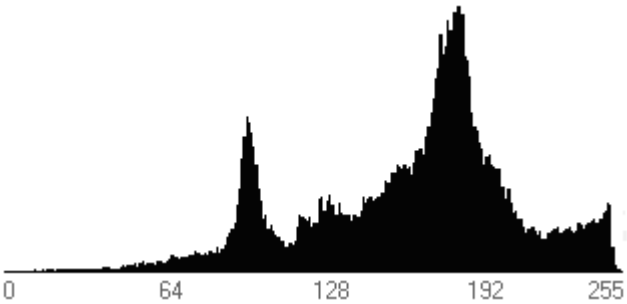

Figure 9. Altered stego-image histogram of the colored image (JPEG)

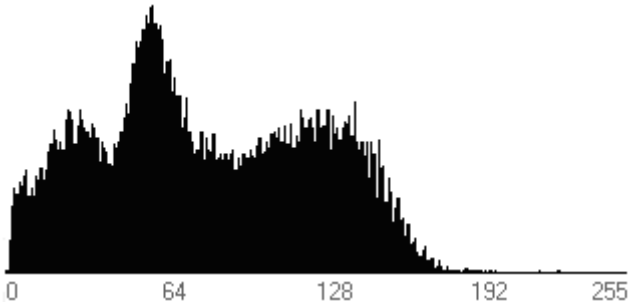

Figure 10. Original image histogram of the colored image (PNG)

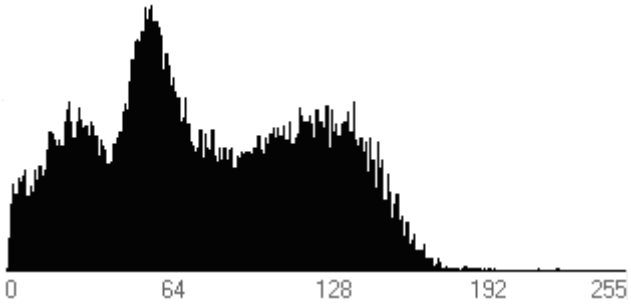

Figure 11. Altered stego-image histogram of the colored image (PNG)

V. CONCLUSION

In conclusion, in an electronic voting system life cycle, the protection of voter's personal information and vote is crucial. It is as important to their rights to verify that their vote has been counted correctly in the tally phase. The proposed algorithm is based on a combination of cryptography and steganography techniques. It would ensure the reliability, security, convenience while offering more efficient election process and it allows the voter to retrieve a receipt for their own verification purpose. Other than that, the electronic voting system implementation could also help the election officials who administer the election to minimize the cost of the election itself. If it is designed properly, the system could actually provide a more secure system than the paper-based election by providing precise data communication and logging, prevention over threats and attacks by the intruders.

REFERENCES

[1] A. Fujioka, T. Okamoto, K. Ohta, "A practical secret voting scheme for large scale elections," Proceedings of the Advances in Cryptology - EUROCRYPT '92, Workshop on the Theory and Application of Cryptographic Techniques, p.244-251, Balatonfüred, Hungary, Dec. 13-16, 1992.

[2] J. Benaloh, "Simple verifiable elections", Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop 2006 on Electronic Voting Technology Workshop, pp.5-5, Vancouver, B. C., Canada, Aug. ,1 2006.

[3] I. Damgârd, "The Theory and Implementation of an Electronic Voting System," in Secure Electronic Voting, D. Gritzalis, Ed. USA: Springer, 2003, vol. 7, pp. 77-98.

[4] J . Benaloh and D. Tunistra, "Receipt-Free Secret-Ballot Elections", Proceedings of the 26th ACM Symposium on Theory of Computing (STOC 1994), pp. 544-553, ACM Press, Montreal, Quebec, Canada, 1994.

[5] M. Hirt, K. Sako, "Efficient Receipt-Free Voting Based on Homomorphic Encryption,'' Advances in Cryptology — EUROCRYPT '00 (B. Preneel, Ed.), LNCS, vol. 1807, pp. 539-556, Springer-Verlag, Berlin, 2000.

[6] C. H. Chen, C. M. Lan, G. Horng, "A practical voting system for small-scale election," Information Technology: Research and Education, 2005. ITRE 2005.3rd International conference, pp. 322-326, Hsinchu, Taiwan, June 27-30, 2005.

[7] L. F. Cranor, R. K. Cytron, "Sensus: a Security-conscious Electronic Polling System for the Internet," System Sciences 1997, Proceedings of the Thirtieth Hawaii International Conference, vol.3, pp.561-570, Wailea, Hawaii, USA, Jan. 7-10, 1997.

[8] D. Chaum, "Secret-ballot receipts: true voter-verifiable elections," IEEE Security and Privacy, vol 2, pp. 38-47, Oakland, California, USA, Jan. 2004.

[9] M. Naor, A. Shamir, "Visual cryptography,'' Cryptology EUROCRYPT'94 (A. DeSantis, Ed.), LNCS, vol. 950, pp. 112, Springer-Verlag, Berlin, 1994.

[10] S. Chandramathi, K. R. Ramesh, R. Suresh, S. Harish, "An overview of visual cryptography," International Journal of Computational Intelligence Techniques, vol. 1, issue 1, pp.32-37, 2010.

[11] R. Z. Wang, "Region Incrementing Visual Cryptography," Signal Processing Letters, IEEE, vol. 16, no. 8, pp. 659-662, Aug. 2009.

[12] N. F. Johnson, S. Jajodia, "Exploring steganography: Seeing the unseen," Computer , vol. 31, no.2, pp.26-34, Feb. 1998.

[13] T. Morkel, J. H. P. Eloff, M. S. Olivier, "An overview of image steganography," Proceedings of the ISSA 2005 New Knowledge Today Conference, pp.1-11, Johannesburg, South Africa, 2005.

[14] P. Vora, "David Chaum's voter verification using encrypted paper receipts," Cryptology ePrint Archive, Report 2005/050, Feb. 2005.

[15] D. A. Gritzalis, "Principles and requirements for a secure e-voting system," Computers & Security, vol. 21, issue. 6, pp.539-556, Oct. 2002.

[16] N. Paul, D. Evans, A. Rubin, D. Wallach, "Authentication for remote voting," Workshop on Human-Computer Interaction and Security Systems, Fort Lauderdale, Florida, April. 5-10, 2003.

[17] L. Langer, A. Schmidt, R. Araujo, "A pervasively verifiable online voting scheme," Informatik 2008 LNI, vol. 133, pp. 457-462, 2008.

[18] A. Shamir, "How to share a secret," Communications of the ACM, vol. 22, no. 11, pp.612-613, 1979.

[19] H. Wei, Z. Dong, C. Ke-fei, "A receipt-free punch-hole ballot electronic voting scheme," Signal-Image Technologies and Internet-Based System, 2007. SITIS 2007. Third International IEEE Conference, pp.355-360, Shanghai Jiaotong University, China, Dec. 16-18, 2007.

[20] N. Provos, P. Honeyman, "Hide and seek: an introduction to steganography," IEEE Security & Privacy, vol.1, no.3, pp. 32- 44, Oakland, California, USA, May-June 2003.