Proposed Adaptive Steganography

Raghad Khalid Mohammed[1], **Woud Majid Abed**[2]

[1]Lecturer, Department of Basic Science, College of Dentistry, University of Baghdad, Iraq

Abstract: ***The definition of steganography is that it is the science of hiding or inserting "data" in transmission media. Its main goals, which are undetectability, robustness and capacity of the embedded data, are the basic elements which make it distinguishable from Cryptography. This paper includes a research on Digital Image with Adaptive Steganography is presented. The issue of steganography has been attacked from two directions. The first method attempts at overcoming the Targeted Steganalytic Attacks. The research is basically focused towards1st order stats based targeted attacks. A couple of specific algorithms have been suggested that are capable of preserving the 1st order statistics of an image post hiding. The second method has the aim of resisting Blind Steganalytic Attacks specifically the attacks that are known as Calibration based Blind Attacks that attempt at estimating a structure of the cover from the steganographic image. A Statistical Hypothesis Test frame-work was established to test the effectiveness of the blind attack. An ordinary frame-work for JPEG steganography was presented that disturbs the cover image structure estimating of the blind attacks. Comparing results prove that the suggested method is capable of successfully resisting the calibration based blind attacks as well as some non calibration based attacks.***

1. Introduction

Since the beginning of the era of Internet, one of the most significant elements of IT and communications has been the data security. Each day, a great deal of data is moved over the Internet via email, file sharing sites, social network sites and so on. Due to the fact that the number of Internet users keeps growing, the idea of Internet security is gaining significance as well [1]. The highly competitive property of the IT industry forces web services to the market at a very high speed, leaving a small amount of time or none at all for auditing the system security [2].

Because of the speedy improvement of communication technology, it's of convenience acquiring multi-media data. However, the issue of illegal data accessing happens continuously and everywhere. Therefore, it's of high importance protecting the contents and the authorized usage of multi-media in the face of attackers. Data encryption is a way of making the data unreadable, imperceptible or impossible to comprehend throughout transmitting via scrambling the contents of the data [3].

In contrast, steganography approaches indicate the techniques of inserting private data into a cover in a way in which people are not capable of discerning that the embedded data exists at all. The image steganography approaches are suggested for hiding the private images into readable but non-critical covers. They're modeled for the reduction of the perception of illegal users. Widely known approaches for steganography may be classified to spatial and transformation domain approaches. In the first one, data hiding is an emerging field of study encompassing implementations like copy-right protecting for digital medium, water-marking, finger-printing, and steganography [4].

In water-marking applications, the message includes data like owner recognition and a digital time stamp, typically applied for copy-right protecting.

In finger-prints, the owner of the dataset inserts a serial code which uniquely recognizes the dataset user. Which adds to copy-right data to make it possible tracing any unauthorized usage of the dataset back to the user.

Steganography hides the private message in the cover dataset and its existence unnoticeable and to be communicated to a receiver in a reliable way. The cover dataset is damaged on purpose, but in a covert manner, modeled to be imperceptible to any data analysis [5].

A Steganography Frame-work

Any steganography system may be researches as depicted in Fig. 1. For a steganography method, that has a steganographic key, considering any cover data the inserting operation produces a steganographic image. The operation of extracting takes the steganographic image and with the use of the shared key applies the inverse algorithm for the extraction of the embedded message [6]. A and B are two inmates needing communication for come up with an escape plan. Still, The Warden detect and check the action of communication among the two parties, W. for sending private data to B, Private message 'm' is inserted by A in the cover 'c', to get the steganographic item 's'. This item is afterwards transmitted via the open communication channel. In a sole steganography structure, the approach to embed the message is not known to W and is known secretly between A and B. In the secret key hiding process, Secret key is shared between the two parties A and B for embedding the message. For instance, the private key may be a pass-word used as a seed for a PRNG for selecting pixel indexes in an image cover to embed the private message. W has no idea concerning the private key which A and B are sharing, even though W knows the approach that they may be using to embed data. In public key steganographic algorithms, A and B have secret-public pairs of keys and are aware of one another's public key. In this paper private key steganography method is the method that has been used [7].

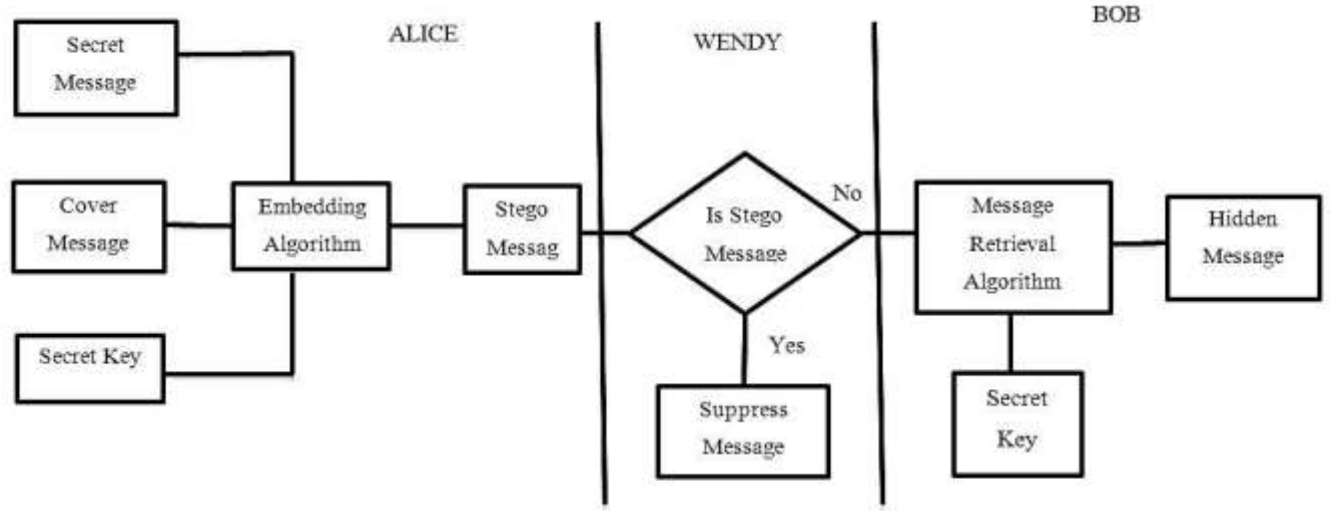


Figure 1: Private Key Passive Steganography [8]

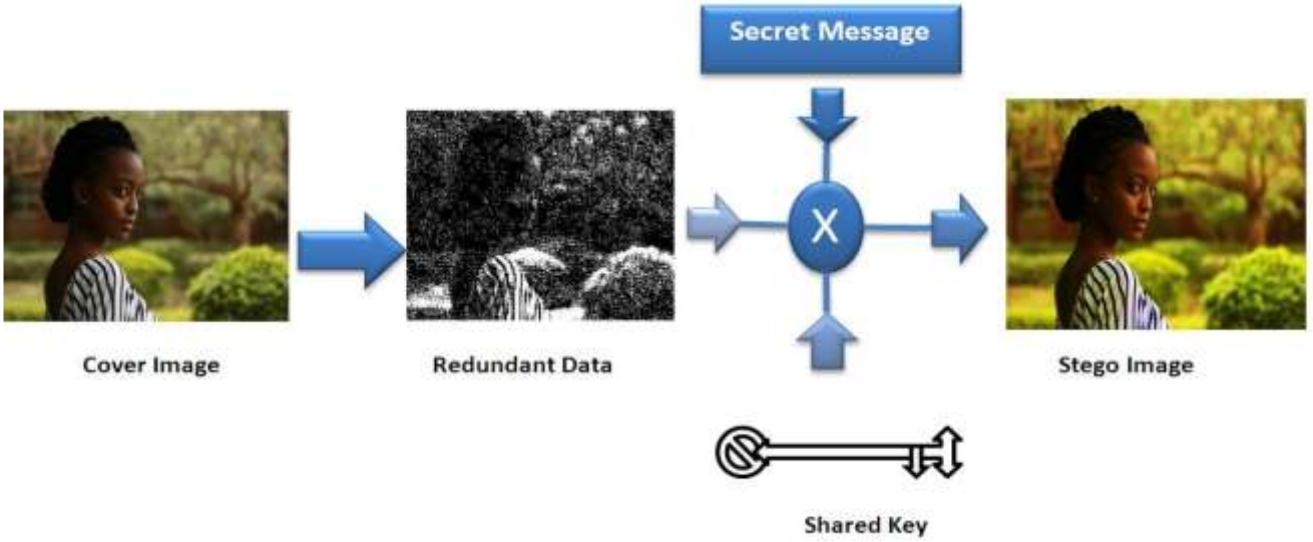


Figure 2: Private Key steganography [9]

2. Statement of the Problem

Steganography is concerned with hiding data in a cover source, in parallel, Stego analysis is the science which detects messages embedded with the use of steganography; which is an analog to cryptographic analysis applied to cryptography [8].

The aim of stego analysis is the identification of suspected packages, determining if they have a payload encoded in them or not, and, preferably, recovering that payload. Therefore, the main issues of efficient steganography are:-

1) The Privacy of Hidden Communication: for the sake of avoiding raising the suspicion of an eavesdropper, while evading the meticulous screening of algorithmic detections, the embedded messages have to be invisible in both of the perceptual and statistical concepts.
2) Size of Payload: in contrast to the water-marking that requires embedding only a little amount of copy-right data, steganography's aim is the hidden communication and thus, typically needs efficient inserting capability. Requirements for higher payload and protected communication are typically contradictory. According to the specified implementation cases, a tradeoff must be sought.

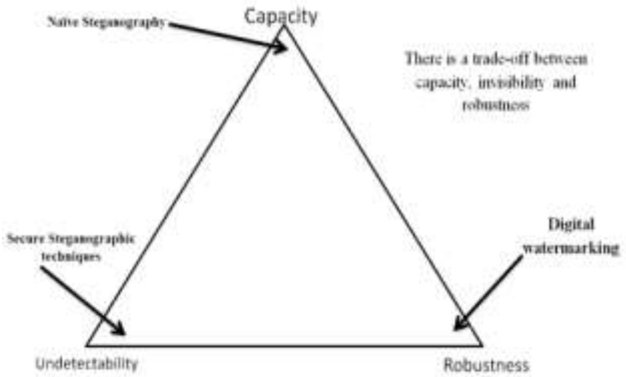

Naive Steganography
Capacity
There is a trade-off between capacity, invisibility and robustness
Secure Steganographic techniques
Digital watermarking
Undetectability
Robustness

Figure 3: Undetectability and robustness in data hiding, Trade-off between embedding capacity

A possible way to categorize the current stego analytic attacks is on the following 2 categories [9]:-

1) Visual Attacks: Those approaches attempt the detection of the existence of data by visually examining it either by the bare eye or via a computer. The attack depends on

trying to guess the embedding layer of an image (for example, a bit plane) and then visually examining that layer to find any suspicious alterations in that layer.

2) Statistic Attacks: Those approaches utilize first or higher order image statistics for revealing little modifications in the statistic behavior resulted from steganography inserting and therefore is capable of successfully detecting even little amounts of embedding with a very high precision. Those class of stego analytic attacks are classified more as "Targeted Attacks" or "Blind Attacks" as explained in detail in the upcoming few sections.

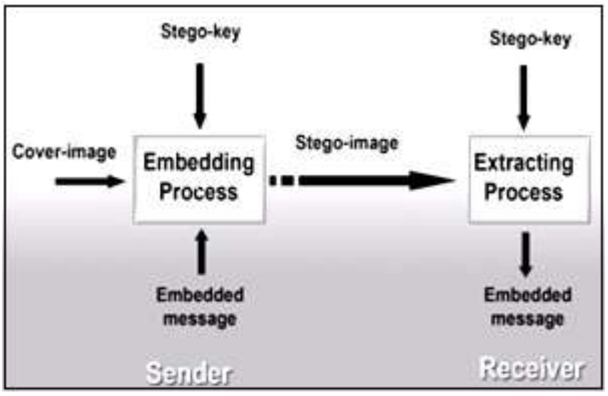


Figure 4: A general steganography frame-work

3. The Proposed Algorithm

An innovative steganographic structure is presented for resisting calibration based blind stego analytic attack. The presented structure that is based on spatial block de-synchronizing for disturbing the efficient prediction of cover image statistics from the steganographic image and that is the main property of the calibration based stego analytic attack. A comparative study with existing steganographic approaches were performed at various embedding rates on the basis of Area under the ROC and Detecting precision. It was discovered that the presented method produced better outputs than the present methods according to detectability against calibration based stego analytic attacks.

The basic goal of the presented method is embedding information in a spatially de-synchronized case of the cover image in a way that the statistics of the cover can't be easily obtained from the steganographic image. Next is a step-wise description of the method.

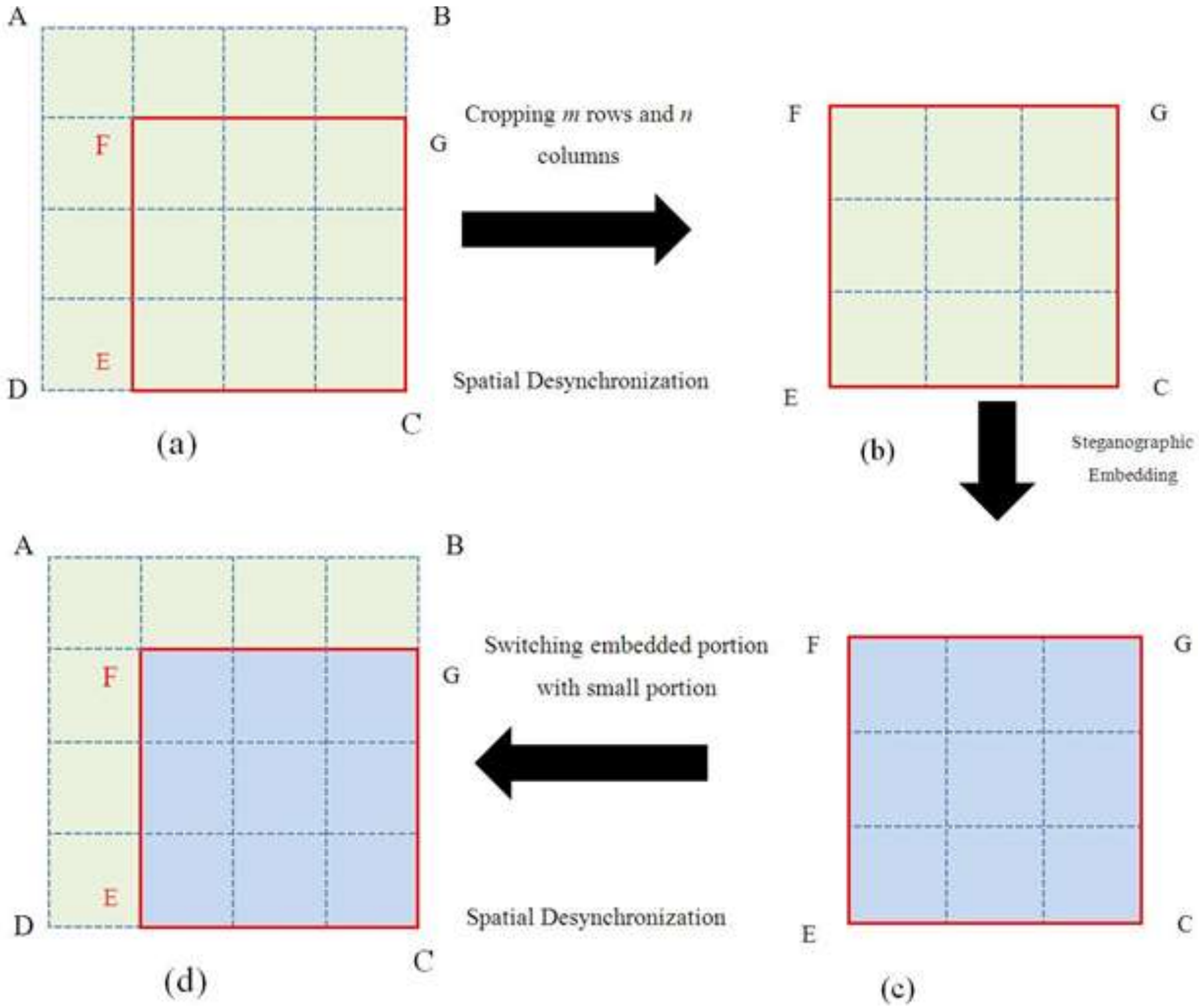

A
B
F
G
E
D
C
(a)
Cropping m rows and n columns
Spatial Desynchronization
F
G
E
C
(b)
Steganographic Embedding
A
B
F
G
E
D
C
(d)
Switching embedded portion with small portion
Spatial Desynchronization
F
G
E
C
(c)

Figure 5: desynchronization used in the proposed Algorithm

Proposed adaptive steganography algorithm

Input: CoverImage I
Input Parameters: Rows & Columns undergo cropping process (u, v), The Block size of (m* n), Quantizing Matrix (Q)
Output: StegoImage Is
Begin

1) split the cover Ì to Î u, v and Ì u, v and Iδ U, V via cropping u top-most rows and v left;-most columns.
2) carry out m × n non-overlapping block partitioning on Î U, V.
3) It should be noted that this collection of blocks by P I u, v (m × n)
4) Select a group of blocks from P Î u, v (m × n) (with the use of a key shared by each one of the two parties) and carry out the inserting in every chosen block with the use of any standard discrete cosine transform based steganography method. The quantizing matrix Q that is a shared secret is utilized to obtain the quantized coefficients.
5) Applying de-quantization and Inverse DCT (IDCT) to the group of blocks that are utilized to embed in Step3.
6) Join Iδ U, V with the resultant image obtained at Step4. This combined image is the resulted steganographic image IS compressed with the use of JPEG compressing and communicated as the steganographic image.
7) End

Due to the fact that the inserted image is compressed JPEG prior to going through the action of communication with the decoding Side, A few of the date bits inserted, could be wasted throughout the process due to the quantizing stage throughout JPEG compressing. This quantizing loss happens for nearly every discrete cosine transform domain embedding scheme. The aim is to circumvent this issue via inserting data basically in the low-frequency coefficients of the discrete cosine transform.

Using Statistical Hypothesis

Table 1: p-value of Rank Sum Testing for 23 DCA

Embedding Rate (bpnc)	QIM p-value	YASS p-value	Proposed algorithm p-value
0.05	2.15x1-8	0.0042	0.1180
0.10	0	2.44x10-4	0.0065
0.25	0	1.12x1024	4.23x10-6
0.50	0	0	7.53x10-10

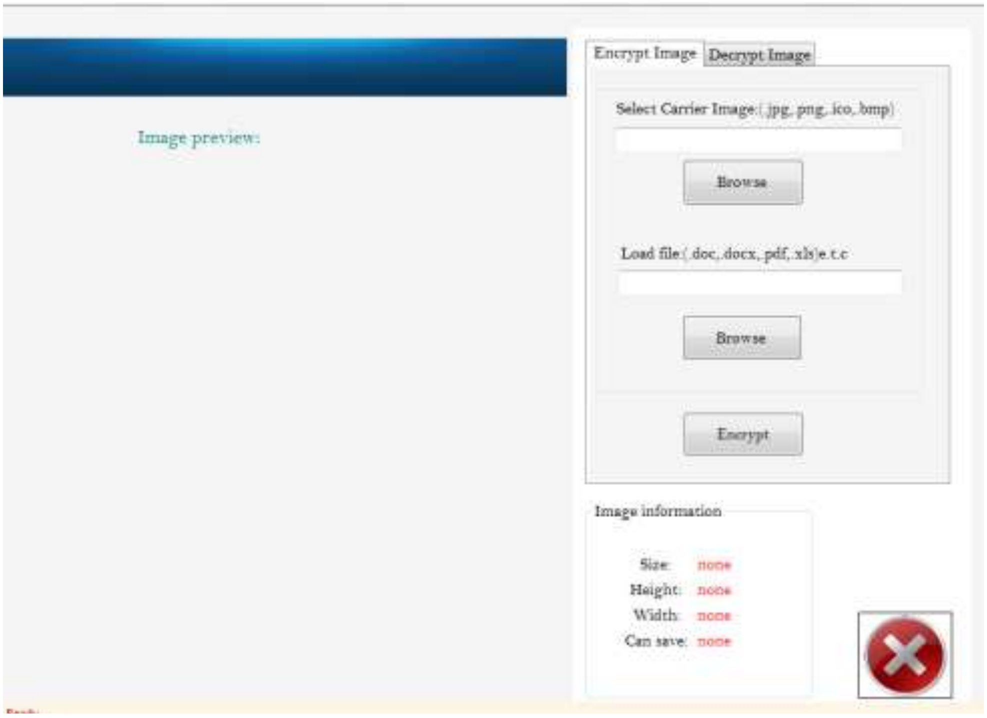
Table 2: p-value of Rank Sum Test for 274 DCA

Embedding Rate (bpnc)	QIM p-value	YASS p-value	Proposed algorithm p-value
0.05	0.1907	0.7947	0.8652
0.10	0.0059	0.6734	0.7853
0.25	1.028x10-16	0.317	0.5213
0.50	0	9.27x10-6	0.3525

It is obvious that for each embedding rate the p-value of the SDSA method is bigger than that of each of the YASS and a QIM scheme which indicates that “SDSA” method construct a steganographic image population that is according to statistics more close to cover image population than all the populations formed by QIM and YASS. Some note need to be taken under consideration and that even though the p values that have been acquired are small but they are high for the process of comparison for the suggested method than that of YASS and QIM.

In this paper a couple of various methods have been explored for steganography. The first one was specified to preserve the marginal statistics of the cover. Preserving marginal statistics helps to defeat the targeted attacks made for specific steganography methods. Two types of algorithms have been discussed under this method. The first one was produced for inherently preserving the first order cover statistics throughout the actual hiding. What has been observed is that this method is capable of resisting the first order statistics based targeted attacks and at the same time preserving a suitable quality of the steganographic image. The second one was a try for an explicit restore of the image marginal statistics after the secret message has been inserted into the image. It has been noted that with a specific constraint the proposed method is the best according to the noise added because of the restoring process. Moreover, it has been noted that even though the restoring of the image statistics may be resistant to targeted attacks, it has no role in improving the security of an embedding method in the face of the blind attacks. This note has been attributed to the fact that the restoring procedure performs as an extra source of noise in the cover which may be captured throughout the process of property extracting and classification. This element minimizes the appropriateness of this method specifically to targeted attacks. The other method that has been researched in this study has the aim to hamper the steg-analyst’s capability for the effective estimation of the stats for the classification. A brand-new statistical design to test the adequacy of calibration based blind attacks has been presented. It has been noted the calibration stage is certainly capable of estimating an image structure. For countering this, a generalized frame-work was presented disturbing this structure attack estimation. It depends on getting the data embedded in a way that that the steganographic population stays statistically closer to cover population and the difference between them can’t be seen in the statistics obtained from the 2 populations. The frame-work has been extended to a new method for JPEG domain hiding. This method has been evaluated in the presented statistic test frame-work and it has been drawn that the method is efficient in resisting the calibration based blind attack.

System views:
In figure 6 the main window of the proposed system is presented where the cover stego message chosen is shown in figure 7 with the image details width, height and size when the chosen message file is successfully inserted to the image a successful notice shows to the user, figure 8



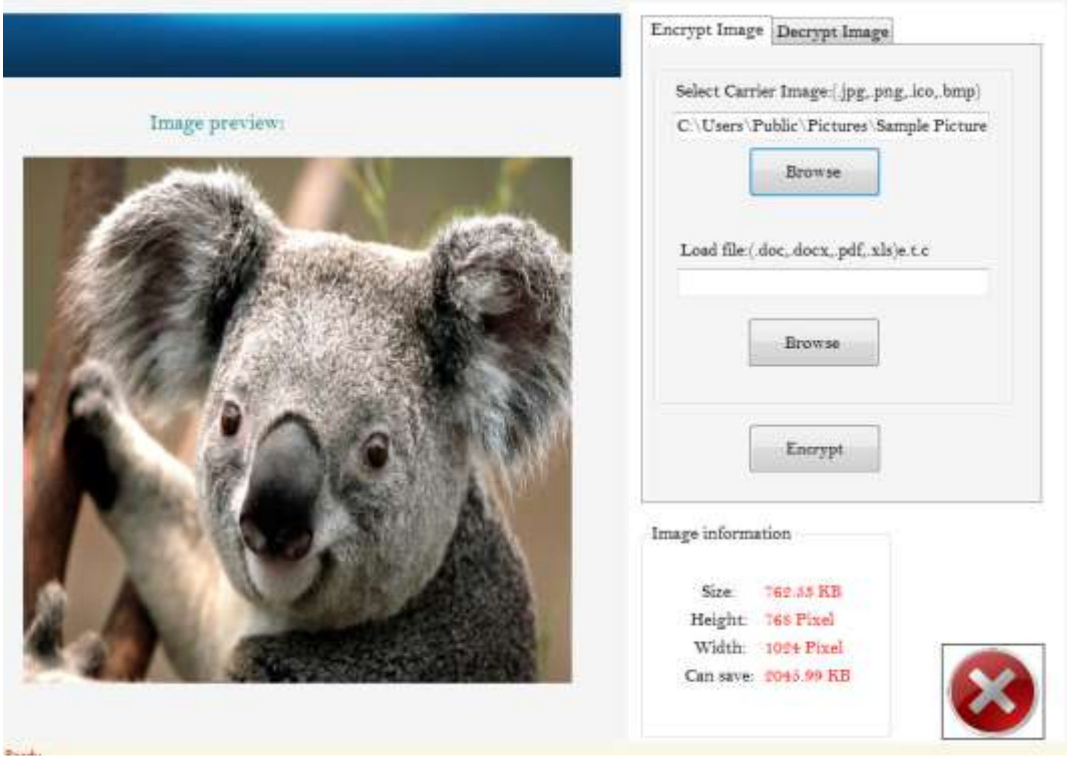
Select Carrier Image:(.jpg,.png,.ico,.bmp)

Load file:(.doc,.docx,.pdf,.xls)e.t.c

Image information

Size: none
Height: none
Width: none
Can save: none

Figure 6: System main window



Select Carrier Image:(.jpg,.png,.ico,.bmp)

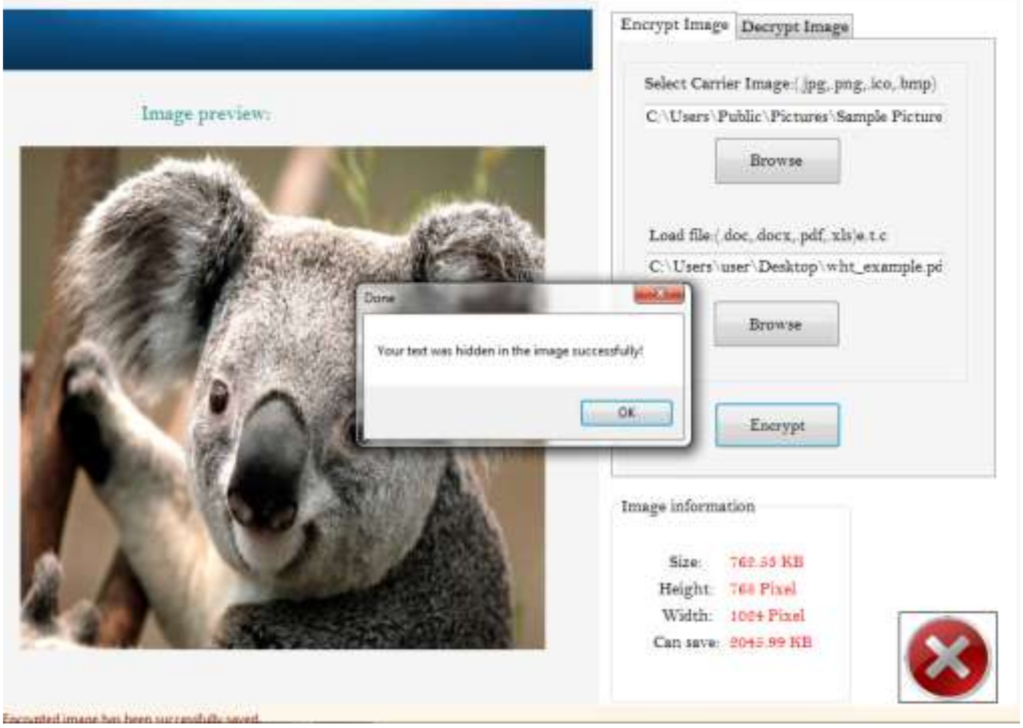
C:\Users\Public\Pictures\Sample Picture

Load file:(.doc,.docx,.pdf,.xls)e.t.c

Image information

Size: 762.53 KB
Height: 768 Pixel
Width: 1024 Pixel
Can save: 2045.99 KB

Figure 7: Stego cover chosen



Select Carrier Image:(.jpg,.png,.ico,.bmp)
C:\Users\Public\Pictures\Sample Picture

Load file:(.doc,.docx,.pdf,.xls)e.t.c
C:\Users\user\Desktop\wht_example.pd

Your text was hidden in the image successfully!

Image information

Size: 762.55 KB
Height: 768 Pixel
Width: 1024 Pixel
Can save: 2045.99 KB

Encrypted image has been successfully saved.

Figure 8: File successfully embedded

4. Conclusions and Future work

The majority of the steganography studies available until now have been aimed toward the design of algorithm that produces steganographic images that are maximally close to the cover data. Every algorithm studies the behavior of the cover at the same timed is missing the message bit series. It is possible designing some encoding functions, which considering a cover image and an inserting method are capable of modifying the message series in a way that it becomes more efficient for embedding than the initial bit series. This type of hiding may be beneficial even in the "Active Warden Framework" of steganography due to the fact that initially, the altered stream will show less noise in the cover. In addition, even in the case where the attacker is familiar with the embedding method, the precise message sequence can only be recreated if the attacker knows the encoding method.

References

[1] A.Joseph Raphael, Dr.V Sundaram, Int. J. Comp. Tech. Appl., Vol 2 (3), 626-630

[2] I. Venkata Sai Manoj, "Cryptography and Steganography", International Journal of Computer Applications (0975 – 8887), Volume 1 – No.12

[3] Jasleen Kour, Deepankar Verma, International Journal of Emerging Research in Management & Technology ISSN: 2278-9359 (Volume-3, Issue- 5)

[4] Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", IEEE Journal of selected Areas in Communications, May 1998 Simmons, G., "The prisoners problem and the subliminal channel", CRYPTO, 1983

[5] Chandramouli, R., Kharrazi, M. & Memon, N., "Image steganography and steganalysis: Concepts and Practice", Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003.

[6] W. J. Chen, C. C. Chang and T. H. N. Le, "High Payload Steganography Mechanism Using Hybrid Edge Detector", Expert Systems with Applications (ESWA 2010), vol. 37, pp. 3292-3301, (2010) April 4.

[7] V. Madhu Viswanatham and J. Manikonda, "A Novel Technique for Embedding Data in Spatial Domain", International Journal on Computer Science and Engineering, IJCSE, vol. 2, (2010).

[8] M. A. Al-Husainy, "Image Steganography by Mapping Pixels to Letters", Journal of Computer Science, vol. 5, no. 1, (2009), pp. 33 -38.

[9] H. Motameni, M. Norouzi, M. Jahandar and A. Hatami, "Labeling Method in Steganography", World Academy of Science, Engineering and Technology, France, (2007).