Volume: 6 Issue: VIII Month of publication: August 2018

DOI:

Secure Communication with Steganography Data Isolation and Analysis

S. Johnrexamalan[1], R. Saravanan[2]
[1] Research Scholar, SCSVMV University, Enathur, Kanchipuram (Tamil Nadu)
[2]Assistant Professor, SCSVMV University, Enathur, Kanchipuram (Tamil Nadu)

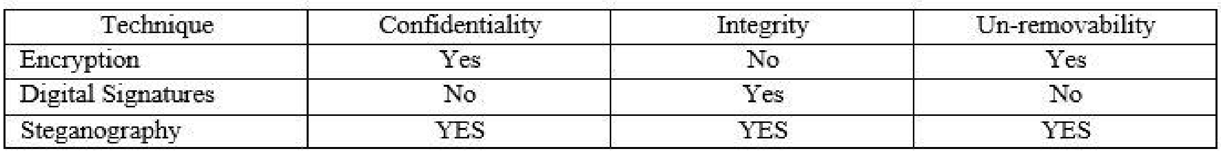
Abstract: Steganography, the craft of concealing messages inside different messages, from security enhanced by cryptography. Presently, steganography is picking up "reputation" with ongoing CIA reports prompting its utilization by psychological oppressor's gatherings and other sorted out wrongdoing syndicates in proclaiming the exchange of mystery data over unmistakable channels to stay away from identification. The point of this paper is to introduce a scholarly research into the field of steganography, or information covering up, as it is some of the time known. And also analyzing the stegano image by using existing forensic tools. We describe method of steganography based on embedding encrypted message bits using AES Algorithm in the 1st least significant (LSB Technique) and last 4 significant bits (Modulus 4 bit technique – LZW Algorithm) of the pixel of image. Here we also provide integrity using MD5 hash algorithm. The analysis shows that the PSNR is improved in the case of LSB technique. Use of hash algorithm provides data integrity.

Keywords: Data hiding, Data integrity, LSB technique, Forensic Analysis, MD5 Hash Algorithm, Substitution, PSNR, Encryption Algorithm, Steganography.

I. INTRODUCTION

To make a steganographic correspondence significantly more secure the message can be packed and scrambled before being covered up in the transporter. Cryptography and steganography can be utilized together [1]. On the off chance that compacted the message will take up far less space in the transporter and will limit the data to be sent. The arbitrary looking message which would come about because of encryption and compression [2] would also be less demanding to stow away than a message with a high level of normality. The picture imprinted on an archive could be commented on by metadata that could lead a client to its high determination variant. By and large, metadata gives extra data around a picture. Despite the fact that metadata can likewise be put away in the record header of a computerized picture, this approach has numerous confinements. Ordinarily, when a document is changed to another format (e.g., from TIFF to JPEG or to BMP), the metadata is lost. So also, editing or some other type of picture control annihilates the metadata [3]. At last, metadata must be connected to a picture as long as the picture exists in the computerized shape and is lost once the picture is printed. Data stowing away enables the metadata to movement with the picture paying little mind to the record configuration and picture state.

TABLE: 1. COMPARISON OF SECURE COMMUNICATION TECHNIQUES



Technique	Confidentiality	Integrity	Un-removability
Encryption	Yes	No	Yes
Digital Signatures	No	Yes	No
Steganography	YES	YES	YES

The main objectives of this work is to provide high level security to sensitive digital data against steganalysis techniques [13]. This objective can be achieved by encrypting and authenticating the image that has user's sensitive data and then embedding the resultant document on to a carrier and to implement proposed model and analysis of the various factors, with less dissertation and improved peak signal noise ratio [10].

In this paper, represents three important techniques based on the algorithm the least significant bit (LSB) [5]. This approach reduces the length of hidden message by LZW algorithm [12] which is a lossless data compression algorithm successor of LZ77 algorithm and the Huffman algorithm. Another important characteristic of this approach is to protect the reduced hidden data by AES (Advanced Encryption Standard) algorithm [9]. Implement the studied approaches on C# which will be easily understandable i.e. user friendly approach. Experiment results and analysis of this paper shows that our improved approach is more effective than existing approaches.

II. PRELIMINARIES A. HASH CODE

A hash work is any capacity that can be utilized to delineate of subjective size to information of a settled size. The qualities returned by a hash work are called hash esteems, hash codes, digests, or just hashes. Hash capacities are regularly utilized as a part of mix with a hash table, a typical information structure utilized as a part of PC programming for fast information query.
Hash capacities quicken table or database query by identifying copied records in an extensive document. One such application is finding comparative stretches in DNA arrangements [14]. They are additionally helpful in cryptography. A cryptographic hash work enables one to effectively confirm that some info information maps to a given hash esteem, yet in the event that the info information is obscure, it is intentionally hard to recreate it (or any proportional options) by knowing the put away hash esteem. This is utilized for guaranteeing honesty of transmitted information, and is the building hinder for HMACs, which give message confirmation.

A. Ansi Table

The ANSI set of 217 characters, otherwise called Windows-1252, was the standard for the center text styles provided with US forms of Microsoft Windows up to and including Windows 95 and Windows NT 4. Amid the lifetime of those two items, Microsoft included the euro cash image bringing the quantity of characters to 218, and presented another center arrangement of Pan- European text styles containing the WGL4 (Windows Glyph List 4) character set, with 652 characters.
The characters that show up in the primary section of the ANSI table are produced from Unicode numeric character references, thus they ought to show up accurately in any Web program that backings Unicode and that has appropriate textual styles accessible, paying little heed to the working framework.

B. LZW Compression

LZW compression is the compression of a document into a littler record utilizing a table-based query calculation designed by Abraham Lempel, Jacob Ziv, and Terry Welch. Two regularly utilized document arranges in which LZW compression is utilized are the GIF picture organize served from Web locales and the TIFF picture design. LZW compression is additionally appropriate for compacting content documents.
A specific LZW compression algorithm takes each info succession of bits of a given length (for instance, 12 bits) and makes a section in a table (once in a while called a "dictionary" or "codebook") for that specific piece design, comprising of the example itself and a shorter code. As information is perused, any example that has been perused before brings about the substitution of the shorter code, successfully packing the aggregate sum of contribution to something littler. Not at all like prior methodologies, known as LZ77 and LZ78, has LZW calculation included the look- into table of codes as a major aspect of the compacted document [15][10]. The translating program that uncompressed the record can manufacture the table itself by utilizing the calculation as it forms the encoded input.

1) *Encoding:* A state perspective of the encoding calculation is appeared here
a) Initialize the word reference to contain all strings of length one.
b) Find the longest string Win the word reference that matches the present info.
c) Emit the dictionary record for W to yield and expel W from the information.
d) Add W took after by the following image in the contribution to the lexicon.
e) Go to Step 2.
2) *Decoding:* The deciphering calculation works by perusing an incentive from the encoded input and yielding the relating string from the initialized dictionary. In order to rebuild the dictionary in the same way as it was built during encoding, it also obtains the next value from the input and adds to the dictionary the concatenation of the current string and the first character of the string obtained by decoding the next input value, or the first character of the string just output if the next value cannot be decoded (If the next value is unknown to the decoder, then it must be the value that will be added to the dictionary this iteration, and so its first character must be the same as the first character of the current string being sent to decoded output).

III. RELATED WORK

This related work survey papers analysing the various proposed approaches that related to steganography and security related issues on existing research works.

The Distortion detection and capacity are compared existing 4 LSB methods according to invisibility benchmark PSNR 30dB is acceptable [4]. In a Substitution-based algorithm, the most immaterial bits of data that decide the important substance of the first document are supplanted with new information in a way that causes minimal measure of contortion. The measure of information that can be covered up is restricted to the measure of immaterial bits in the record.

Higher "quality" records have a tendency to contain more bits of irrelevant data. Straightforward change from a to each other record configuration can demolish the concealed data in the picture. At the point when applying 4LSB methods to every byte of 8-bit picture, one piece can be encoded to every pixel. Any adjustments in the pixel bits will be indistinguishable to the human eye. In order to defeat the steganalytic attacks, algorithms have been proposed which try to restore the statistics whichget distorted during the embedding procedure and which may be used for steganalysis.

Since BMP uses compression, LSB makes use of BMP image. To be able to hide a secret message inside a BMP file, one would require lossless a very large cover image. BMP images of 800 × 600 pixels found to have less web applications [8]. The embedding quality of the stego image is measured by a well-known method, namely peak-signal-to- noise-ratio (PSNR) [11]. It is used to assess the degree of similarity between a stego image and the original image.

There are four calculations as of now executed, each utilization slightest huge piece steganography and some channel the picture first.

A. Blindhide

This is the easiest method to conceal data in a picture. It aimlessly stows away in light of the fact that it just begins at the upper left corner of the picture and works its way over the picture (at that point down - in check lines) pixel by pixel. As it comes it changes the slightest noteworthy bits of the pixel hues to coordinate the message. To disentangle the procedure the slightest critical bits beginning at the upper left are perused off. This isn't exceptionally anchor - it's extremely simple to peruse off the slightest critical bits.

B. Hide Seek

This calculation arbitrarily circulates the message over the picture. It is named after "Hide and Seek" – a Windows 95 steganography instrument that uses a comparable method. It utilizes a secret word to produce an irregular seed, at that point utilizes this seed to pick the main position to stow away in. It proceeds to arbitrarily create positions until the point that it has wrapped up the message. It's somewhat more brilliant about how it covers up on the grounds that you need to attempt each blend of pixels in each request to attempt and "split" the calculation. It's as yet not the best strategy since it isn't taking a gander at the pixels it is stowing away.

C. Filter First

This algorithm filters the image using one of the inbuilt filters and then hides in the highest filter values first. It is basically a fancier rendition of Blind Hide.

D. Battle Steg

This calculation performs "Battleship Steganography". It first channels the picture at that point utilizes the most elevated channel esteems as "ships". The calculation then haphazardly "shoots" at the picture (like in Hide Seek) and when it finds a "ship" it groups its shots around that hit in the expectation of "sinking" the "ship". Sooner or later it moves away to search for different boats. The impact this has is that the message is arbitrarily covered up, however frequently covered up in the "best" parts to stow away in on account of the boats. It moves away to search for different ships with the goal that we don't debase a zone of a picture too significantly.

E. Dynamic Battlesteg & Filter First: These Two Calculations Do Likewise As Battlesteg

And Filter First, with the exception of they utilize dynamic programming to influence the stowing away to process quicker and less memory serious. They are NOT good with the first calculations in light of the fact that the request of pixels kept in the dynamic cluster isn't precisely the same.

IV. PROPOSED METHOD

The basic idea behind the image steganography is that to ensure the secure communication between two. Many stenographic methods compress only the data. With this proposed architecture the compression should take place on both ends. In image compression make use of repeated bits.

Proposed architecture indicates that there was two kind of compression that have been made. With this image compression part there are many compression algorithms used for it, so there we cope with the existing compression style of 64-bit conversion [14]. In another hand text file compression has to be effective for the distortion ratio.

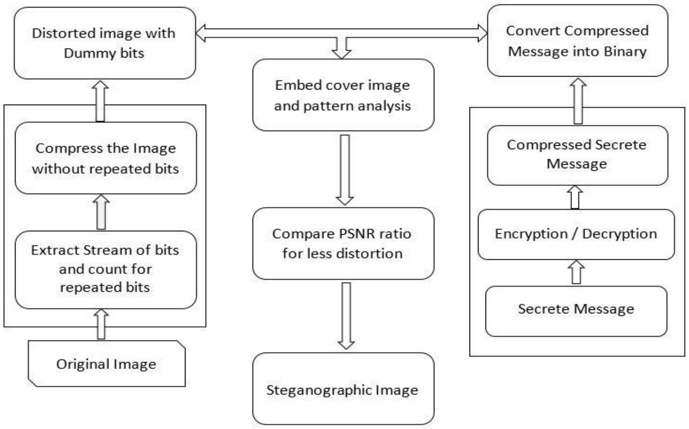

Distorted image with Dummy bits
Compress the Image without repeated bits
Extract Stream of bits and count for repeated bits
Original Image
Embed cover image and pattern analysis
Compare PSNR ratio for less distortion
Steganographic Image
Convert Compressed Message into Binary
Compressed Secrete Message
Encryption / Decryption
Secrete Message

Figure 1: Proposed Architecture

The LZW Compression Algorithm is utilized to break down information and decide how to decrease the measure of that information by supplanting repetitive data with metadata. Areas of the information that are In distinguishable information have been encoded are supplanted by a little measure of metadata shows how to grow those segments [6]. The encoding calculation is utilized to take that mix of information and metadata and serialize it into a flood of bytes that can later be decoded and decompressed.

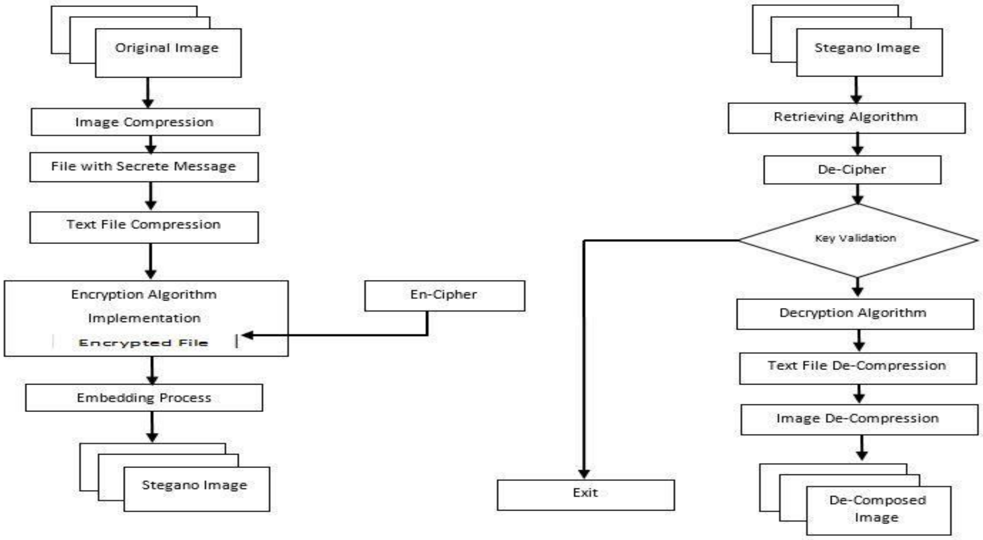


Figure 2: Flow Diagram

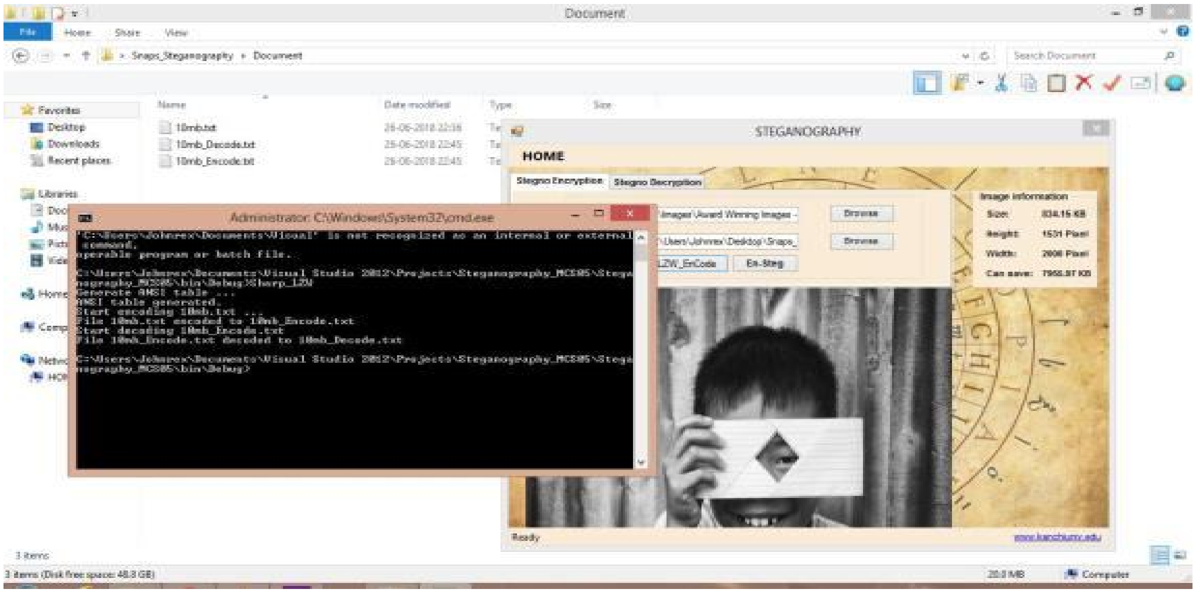
After the compression the text file will be encrypted with the encryption algorithm. For the encryption process the cipher text will be passed by hash, so that the length of the cipher text cannot impact the file size for resulted stego image [7]. After encryption the image and text file must be embedded using the embedding algorithm [5], which make sure file is not detectable. In the receivers end the process take a reverse action. And make sure the file has a correct coordinates with lesser impact.

A. *Working Principle*

1) Step 1: Prepare image for steganography, by using the compressed dump space in image.
2) Step 2: Once image prepared, do a LZW compression to compress text file and changes text file as hash. It converts bits.
3) Step 3: Give a valid name for saving the stego bitmap image. (Using bitmap for distortion. Image can't easily broke).
4) Step 4: Final resulted image with secrete message served to the end user.
5) Step 5: For De-Steg take the same steps just reverse.
6) Step 6: User review and comment by contact page.

V. RESULTS AND ANALYSIS

In this work, approached steganography algorithm for a hidden message inside a cover- image, all these algorithms based on the LSB technique. However, we propose an improved method which is based on combination between LSB4 (Bit Substitution Technique) Encoding technique and cryptographic algorithm. To evaluate the performance the algorithm, software application have been implement in visual studio using C#. Using the studied algorithms, we have successfully hide a message in a carrier image. And compare the studied techniques with our approach in terms of hex code comparison and various stegaoanalysis tools for the distortion ration between the original image and the stego-image.



Name	Date modified
10mb.txt	25-06-2018 22:38
10mb_Decode.txt	25-06-2018 22:45
10mb_Encode.txt	25-06-2018 22:45

Image information

Size:	834.15 KB
Height:	1531 Pixel
Width:	2808 Pixel
Can save:	7955.87 KB

Administrator: C:\Windows\System32\cmd.exe

```
'C:\Users\Johnrex\Documents\Visual' is not recognized as an internal or external
 command,
operable program or batch file.

C:\Users\Johnrex\Documents\Visual Studio 2012\Projects\Steganography_MCS85\Stega
nography_MCS85\bin\Debug>Sharp_LZW
Generate ANSI table ...
ANSI table generated.
Start encoding 10mb.txt ...
File 10mb.txt encoded to 10mb_Encode.txt
Start decoding 10mb_Encode.txt
File 10mb_Encode.txt decoded to 10mb_Decode.txt

C:\Users\Johnrex\Documents\Visual Studio 2012\Projects\Steganography_MCS85\Stega
nography_MCS85\bin\Debug>
```

3 items
3 items (Disk free space: 48.8 GB)

Figure 3: Steganography Application

The steganography image based text hiding aimed to create application with lesser distortion ratio. The main influencing factor for stago-analysis is directory attack. Major techniques like JP Hide & Seek, StegDetect.

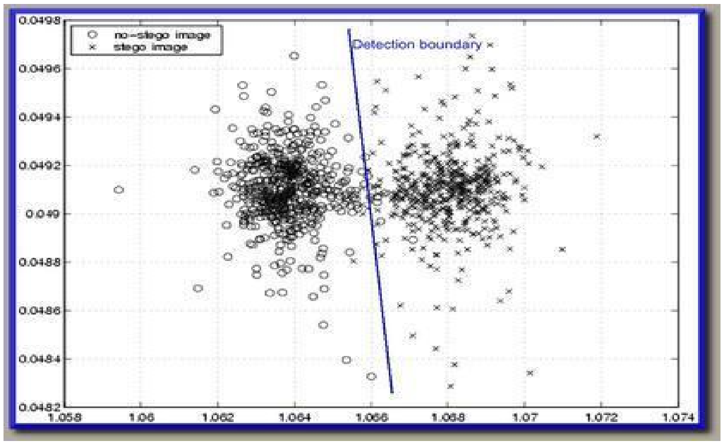
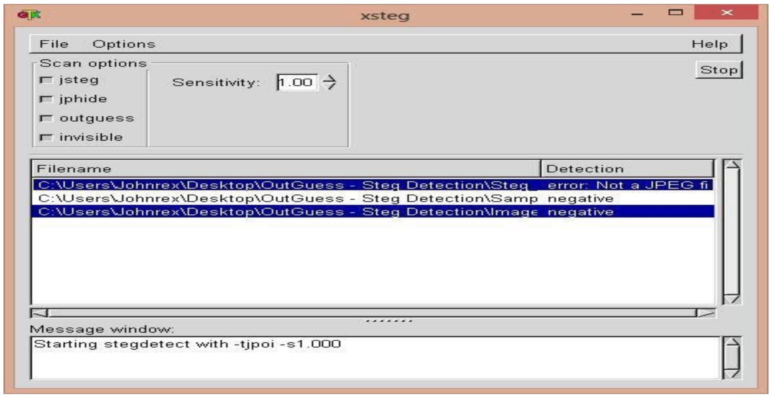


Figure 4: Directory Detection Boundary

Given an arrangement of typical pictures and an arrangement of pictures that contain concealed substance by another steganographic application, Stegdetect can consequently decide a direct identification work that can be connected to yet unclassified pictures.

```
$ stegdetect          *.jpg
Image_Hide.jpg  : outguess(old)(***) jphide(*) Steg_1.bmp  : error: Not a JPEG file: starts with
0x89 0x50
Sample3.jpg : jphide(***)
Sample4.jpg       : negative
 [...]
$ stegbreak -tj dscf0002.jpg
Processed 1 files, found 1 embeddings. Time: 36 seconds: Cracks: 324123, 8915 c/s
```

Table 2: Stegdetect Image Analysis



Scan options
□ jsteg
□ jphide
□ outguess
□ invisible

Sensitivity: 1.00

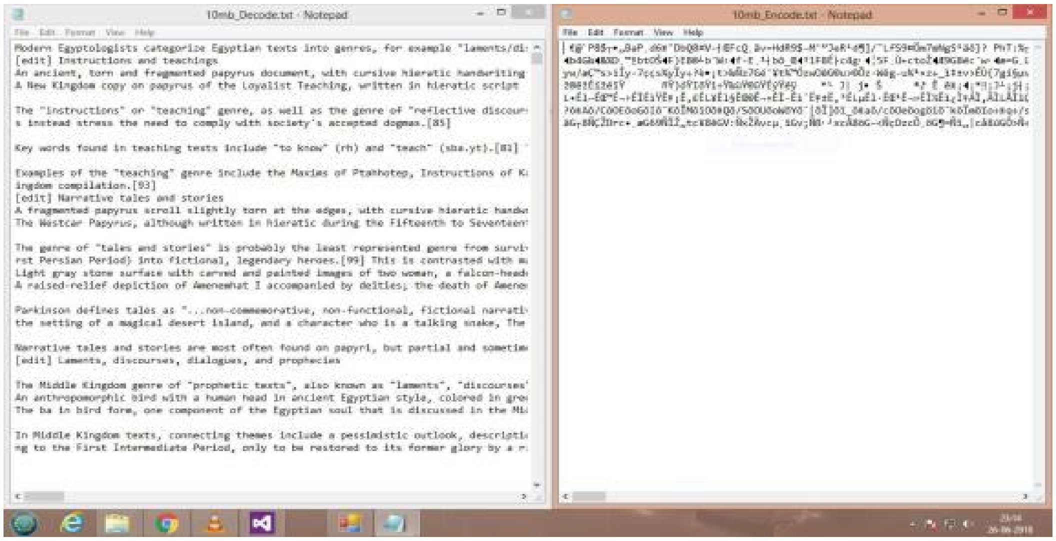
Filename	Detection
C:\Users\Johnrex\Desktop\OutGuess - Steg Detection\Steg	error: Not a JPEG fi
C:\Users\Johnrex\Desktop\OutGuess - Steg Detection\Samp	negative
C:\Users\Johnrex\Desktop\OutGuess - Steg Detection\Image	negative

Message window:

```
Starting stegdetect with -tjpoi -s1.000
```

Figure 5: Stegdetect Analysis

Stegdetect can discover concealed data in JPEG pictures utilizing such steganography plots as F5, Invisible Secrets, JPHide, and JSteg (OutGuess 2003).


10mb_Decode.txt - Notepad
File Edit Format View Help
10mb_Encode.txt - Notepad
File Edit Format View Help

```
Modern Egyptologists categorize Egyptian texts into genres, for example "laments/di:
[edit] Instructions and teachings
An ancient, torn and fragmented papyrus document, with cursive hieratic handwriting
A New Kingdom copy on papyrus of the Loyalist Teaching, written in hieratic script

The "instructions" or "teaching" genre, as well as the genre of "reflective discour
s instead stress the need to comply with society's accepted dogmas.[85]

Key words found in teaching texts include "to know" (rh) and "teach" (sba.yt).[81]

Examples of the "teaching" genre include the Maxims of Ptahhotep, Instructions of K
ingdom compilation.[93]
[edit] Narrative tales and stories
A fragmented papyrus scroll slightly torn at the edges, with cursive hieratic handw
The Westcar Papyrus, although written in hieratic during the Fifteenth to Seventeen

The genre of "tales and stories" is probably the least represented genre from survi
rst Persian Period) into fictional, legendary heroes.[99] This is contrasted with m
Light gray stone surface with carved and painted images of two woman, a falcon-head
A raised-relief depiction of Amenemhat I accompanied by deities; the death of Ameno

Parkinson defines tales as "...non-commemorative, non-functional, fictional narrati
the setting of a magical desert island, and a character who is a talking snake, The

Narrative tales and stories are most often found on papyri, but partial and sometim
[edit] Laments, discourses, dialogues, and prophecies

The Middle Kingdom genre of "prophetic texts", also known as "laments", "discourses'
An anthropomorphic bird with a human head in ancient Egyptian style, colored in gre
The ba in bird form, one component of the Egyptian soul that is discussed in the Mi

In Middle Kingdom texts, connecting themes include a pessimistic outlook, descripti
ng to the First Intermediate Period, only to be restored to its former glory by a r
```

Figure 6: Hidden Text File Analysis

Comparing the original text file with decoded file shows that the encoding or compression process didn't affect the text. There is no changes in the decoded document. At another end the comparison between encoded and decoded text files shows that the entire text body is hash coded.

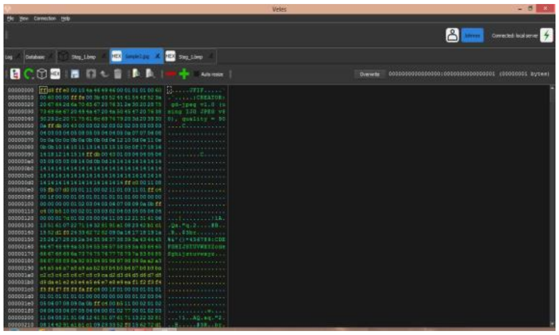


Figure 7: Hex Code Analysis – Original Image

Image hex code analysis make sense with the original image and stegao image or fragmented image. Using the "Veles Application" here at below can find resulted bits. The stego image has many green area, means that the image file has been de-fragmented by the application we use to do steganography.

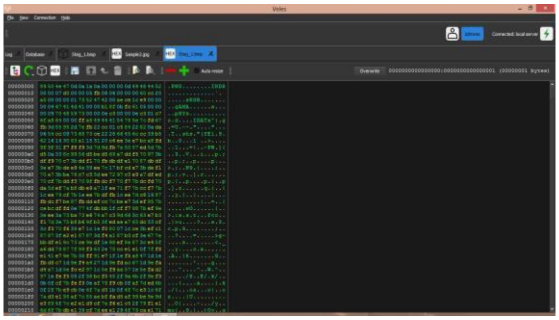


Figure 8: Hex Code Analysis – Stego Image

VI. CONCLUSION

Now a day's modern generation cope with new technologies. And the world changes with digitalized. So network security plays major role, this paper concludes the same. The software or applications are coming forth with various functionalities. And security makes a big question mark. In future every transaction or transcription needs security that secures end to end communication. So this research work find a way to high on cryptography, steganography make possible outcomes with modern day security.

Steganography made vulnerable by steg-analysis. There are many applications provide steganography. But in other side there are plenty of applications that finds the stegano images with some directory attacking. And possibly modify the application with some virus so that the security has been compromised. For this kind of operations we could use proposed application, which has high possibilities with not-detectable. With various analysis we come to this conclusion that the proposed application "Secure Communication with Steganography Data Isolation" can make a difference with existing steganography application.

A. *Feature Work*

1) Even though special improvements with the proposed mechanism, the file size of stegano object has the drawback. So with this the future research work may conclude.
2) As per the security crises, steganography can be implemented with web-based communications. Such as bank transactions, military communications. The research work in future may enhance the internet protocols.
3) Various types of security measurements like directory poisoning, Bit location finder, Length Measurement. Those all kind of security threads can be detected and concealed.

REFERENCES

[1] Sarita Kumari, "A research Paper on Cryptography Encryption and Compression Techniques" International Journal of Engineering and Computer Science ISSN: 2319-7242 Volume 6 Issue 4 April 2017, Page No. 20915-20919.

[2] Johnson and Jajodia, "Exploring Steganography: Seeing the Unseen", Center for Secure Information Systems, Dept. of Information and Software Systems Engineering, George Mason University.

[3] V.Saravanan and A.Neeraja, "Security Issues in Computer Networks and Stegnography", Proceedings of7'h International Conference on Intelligent

Systems and Control (ISCO 2013), 978-1-4673-4603-0/12/$31.00 ©2012 IEEE.

[4] S. K. Moon and R.S. Kawitkar, "Data Security using Data Hiding", IEEE International conference on computational intelligence and multimedia applications, vol. 4, pp. 247-251, Dec. 2007.

[5] Vinod Parihar, Devanshu Gehlot, “A Steganography Implementation based on LSB & LDR Algorithm”, Master of Science, Cyber Security Students SPUP, Jodhpur.

[6] Siva Shankar.S, Dr.Rengarajan.A, “Puzzle based Highly Secure Steganography”, Bharath University, Selaiyur, Chennai, India. Department of CSE VelTech MultiTech Dr.RR Dr.SR Engineering College, Avadi, Chennai, India.

[7] Qiangfu Zhao, Tosiyasu L. Kunii, “Steganography Based on Image Morphing”, Dept. of Computer and Information Systems, The University of Aizu, Aizuwakamatsu, Fukushima, Japan.

[8] Beenish Mehboob and Rashid Aziz Faruqui, “A Stegnography Implementation”, -4244-2427-6/08/$20.00 ©2008 IEEE , Department of Computer Science and Engineering Bahria University, Karachi, Pakistan.

[9] Sofyane Ladgham Chikouche, Noureddine Chikouche, “An Improved Approach for LSB- Based Image Steganography using AES Algorithm”, 978-1-5386-0686-5/17/$31.00 ©2017 IEEE, The 5th International Conference on Electrical Engineering – Boumerdes (ICEE-B) October 29-31, 2017, Boumerdes, Algeria

[10] Deshpande Neeta, Kamalapur Snehal, “Implementation of LSB Steganography and Its Evaluation for Various Bits”, Computer Science Dept, K.K.Wagh Institute of Engineering Education & Research, Nashik, India.

[11] Rupesh Gupta, Dr.Tanu Preet Singh, “New Proposed Practice for Secure Image Combing Cryptography Stegnography and Watermarking based on Various Parameters”, 978-1-4799-6629-5/14/$31.00c 2014 IEEE, 2014 International Conference on Contemporary Computing and Informatics (IC3I).

[12] Made Sumarsana Adi Putra, Gelar Budiman, Ledya Novamizanti, “Implementation of Steganography using LSB with Encrypted and Compressed Text using TEA-LZW on Android”,978-1-4799-4575-7/14/$31.00 c 2014 IEEE, 2014International Conference on Computer, Control, Informatics and Its Applications.

[13] Abbas Cheddad, Joan Condell, Kevin Curran, Paul McKevitt, “Digital image steganography: Survey and analysis of current methods”, Signal Processing 90 (2010)727–752, doi:10.1016/j.sigpro.2009.08.010

[14] J. Fridrich, D. Soukal, and M. Goljan, "Maximum likelihood estimation of secret message length embedded using pmk steganography in spatial domain", Proc. of IST/SPIE Electronic Imaging: Security, Steganography, and Watermarking of Multimedia Contents VII, vol.5681, pp. 595-606, 2005.

[15] Marin, G.A., "Network security basics," Security & Privacy, IEEE , vol.3, no.6, pp. 68-72, Nov.-Dec. 2005.