Steganography Techniques: A Review Paper

Mohammad Ajman Hossain[1], Shadi M.S. Hilles[2]

[1]*Faculty of Computer and Information Technology, Al-Madinah International University, Malaysia,* ajmanhossain@gmail.com
[2]*Faculty of Computer and Information Technology, Al-Madinah International University, Malaysia,* shadihilless@gmail.com

Received 30 June 2017; accepted 30 October 2017

Abstract

Steganography is the covering up of a message inside a conventional message. Steganography makes cryptography a stride more distant by concealing a scrambled message so that nobody presumes it exists. Anybody examining information will neglect to know it contains encoded information. Data is very to disseminate over the world effortlessly and financially by the development of innovation and having the quick access of Internet which also made individuals to stress over their protection and works. The steganography give strategies that helps to stow away and blend data inside other data which makes hard to perceive by assailants. The exponential development and secret correspondence of potential users over the web makes the steganography significant. Steganography is accomplished in correspondence, picture, content, voice or media content for copyright, military correspondence, confirmation and numerous different purposes. In picture Steganography, secret correspondence is accomplished to install a message into cover picture and create a stego-picture. By using this innovative technology, the end client get the information as a picture without anybody realizing that the picture contains some basic data, so if the picture is translated by any outsider, the information won't show to them, thus the information will secure amid transmission and the client utilizes a safe code to recover the information from the picture on the receiving end. In this paper diverse Steganography methods for Text, Image, Audio and video Steganography, DCT, DWT, DFT, and furthermore application of Steganography for concealing content will be discussed. This paper gives some vital data about steganography strategies that will help in future looks into in steganography and information concealing field.

Keywords: Text, Image, Audio, video Steganography, DCT, DWT, DFT.

1. Introduction

Steganography is the covering up of a message inside a conventional message. It is a Greek word which signifies "concealed written work". It is characterized into two sections: Steganos which signifies "mystery or secured" and the graphic which signifies "expressing the content". The significance of Steganography is concealing content or mystery messages into another media document, for example, picture, content, sound, and video [1][2][3].

The target of steganography is to refrain from drawing in uncertainty to the nearness of a covered message. This approach of data concealing strategy has as of late turned out to be critical in various application territories. Advanced sound, video, and pictures are progressively outfitted with recognizing yet subtle imprints, which may contain a hidden copyright notice or serial number or even help to forestall unapproved duplicating straightforwardly [4].

Data stowing away is a developing exploration zone, which includes applications, for example, copyright assurance for advanced media, watermarking, fingerprinting, and steganography. Every one of these utilizations of data stowing away are very differing [5].

The fast development of distributing and broadcasting innovation additionally require an option arrangement secluded from data. The copyright for sound, video and other source available in mechanized edge may incite tremendous scale unapproved recreating. This is on the grounds that the computerized groups make conceivable to give high picture quality even under multi-replicating. Hence, the uncommon piece of undetectable data is settled in each picture that couldn't be effectively separated without particular method sparing picture quality [6].

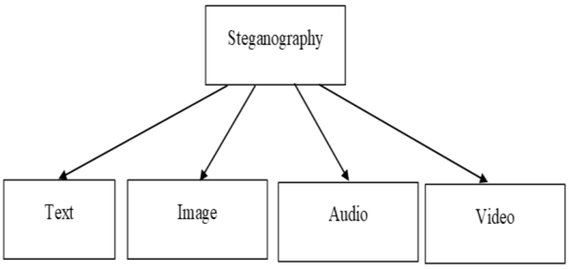

Fig. 1. Different approaches of Steganography

2. Ease of Use

Steganography can be characterized into picture, content, sound and video steganography relying upon the cover media used to install mystery information. Content steganography can include anything from changing the arranging of a current content, to changing words inside a content, to producing arbitrary character successions or utilizing setting free sentence structures to create meaningful writings [7]. Content or Text steganography can be comprehensively grouped into three sorts Format based, Random and Statistical generation, and Linguistic methods [8] [9].

2.1. FORMAT BASED METHODS

This technique utilizes the physical designing of content as a space in which to conceal data. Inclusion of spaces or non-showed characters, cautious mistakes tinny all through the content and resizing of textual styles are a portion of the many organization based strategies utilized for steganography. Some of these strategies, for example, ponder incorrect spellings and space inclusion, may trick human pursuers who disregard periodic incorrect spellings, however can regularly be effortlessly recognized by a PC [10].

This technique has certain imperfections. On the off chance that the stego record is opened with a word processor, incorrect spellings and additional blank areas will get identified. Changed text styles sizes can stimulate doubt to a human pursuer. Furthermore, if the first plaintext is accessible, contrasting this plaintext and the suspected stenographic content would make controlled parts of the content very unmistakable [7].

2.2. RANDOM AND STATISTICAL GENERATION

Random and Statistical Generation strategies are utilized to produce cover-message naturally as indicated by the factual properties of dialect. These techniques utilize illustration syntaxes to deliver cover-message in a specific regular dialect. A probabilistic setting free punctuation is a regularly utilized dialect demonstrate where every change run of a setting free linguistic use has a likelihood related with it [10].

Keeping in mind that the end goal to stay away from examination with a known plaintext, stenographers regularly turn to producing their own cover writings [7]. One technique is hiding data in arbitrary looking arrangement of characters. In another strategy, the factual properties of word length and letter frequencies are utilized as a part of request to make words which will seem to have same measurable properties as genuine words in the given dialect [11].

2.3. LINGUISTIC METHODS

Etymological steganography particularly considers the phonetic properties of created and changed content, and as a rule, utilizes semantic structure as the space in which messages are shrouded [12]. This steganography method particularly considers the phonetic properties of created and adjusted content, and most of the time, utilizes semantic structure as the space in which messages are concealed [7]. CFG make tree structure which can be utilized for disguising the bits where left branch speaks to "0" and right branch compares to '1'. A language structure in GNF can likewise be utilized where the principal decision in a creation speaks to bit 0 and the second decision speaks to bit 1. This technique has a few disadvantages. Initial, a little language structure will prompt part of content redundancy. Besides, despite the fact that the content is grammatically perfect, yet there is an absence of semantic structure. The outcome is a series of sentences which have no connection to each other [7].

3. Image Steganography

Before Image or Picture steganography is the way toward concealing the touchy data into the cover picture with no corruption of the picture and giving better security so that unapproved client can't get to the shrouded data. Figure 2 demonstrates the different picture steganography systems. Picture steganography methods are extensively ordered into taking after:

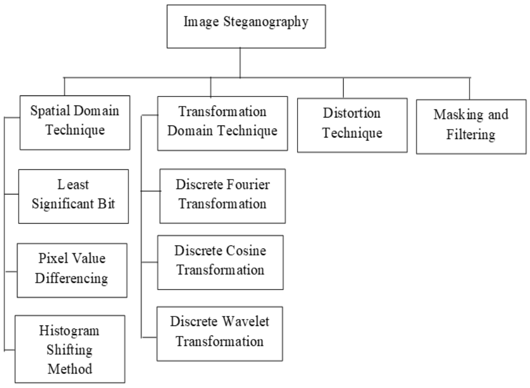
Image Steganography
Spatial Domain Technique
Transformation Domain Technique
Distortion Technique
Masking and Filtering
Least Significant Bit
Pixel Value Differencing
Histogram Shifting Method
Discrete Fourier Transformation
Discrete Cosine Transformation
Discrete Wavelet Transformation

Fig. 2. Various Image Steganography Techniques.

1.1. Spatial Domain Methods

Define In spatial area steganography technique, for concealing the information a few bits are straightforwardly changed in the picture pixel esteems. There are numerous variants of spatial steganography, all straightforwardly change a few bits in the picture pixel esteems sequestered from information. LSB based steganography is one of the most straightforward methods that shrouds a message in the LSBs of pixel esteems without presenting numerous noticeable twists. Changes in the estimation of the LSB are impalpable for human eyes. Spatial area methods are comprehensively characterized into:

- Least significant bit (LSB)
- Pixel value differencing (PVD)
- Edges based data embedding method (EBE)
- Random pixel embedding method (RPE)
- Mapping pixel to hidden data method
- Histogram shifting methodsunavoidable.

1.2. Transformation Domain Technique

This is a more intricate method for concealing data in a picture. Different calculations and changes are utilized on the picture to shroud data in it. Change space installing can be named as an area of inserting procedures for which various calculations have been recommended [13]. The way toward inserting information in the recurrence space of a flag is significantly more grounded than implanting rule that work in the time area. The greater part of the solid stenographic frameworks today work inside the change space Transform area procedures have preference over spatial space strategies as they conceal data in zones of the picture that are less presented to pressure, editing, and picture preparing. Some change space systems don't appear to be subject to the picture arrangement and they may beat lossless and lossy configuration transformations. Change area systems are extensively characterized into:

- Discrete Fourier Transformation Technique (DFT)
- Discrete Cosine Transformation Technique (DCT)
- Discrete Wavelet Transformation Technique (DWT)

Discrete Fourier transformation technique (DFT)

In DFT all the addition of concealed message is done in the recurrence area. It is a more perplexing method for concealing message into recurrence space of the picture. The Discrete Fourier Transform of spatial esteem f (x, y) for a picture of size M × N is characterized in condition for recurrence space change [14].

$$f(u,v) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) e^{-12V \frac{ux}{M} + \frac{vy}{N}}$$

Number So, also IDFT or Inverse Discrete Fourier Transform is utilized to change over recurrence segment of every pixel incentive to the spatial space esteem and the condition for change from recurrence to spatial area is When DFT is connected it changes over the cover picture from spatial space to recurrence space and every pixel in spatial space is changed into two sections: genuine and fanciful part.

$$f(x,y) = \frac{1}{\sqrt{MN}} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} f(u,v) e^{12V \frac{ux}{M} + \frac{vy}{N}}$$

The shrouded message bits are embedded in genuine piece of recurrence space barring first pixel. In the wake of installing IDFT is performed recurrence space changed over into spatial area. Amid the extraction or interpreting of the message picture from spatial space is changed to recurrence area. In the time of applying DFT and extraction calculation the first source picture is recovered.

Discrete Cosine Transformation Technique (DCT)

This change system is valuable for isolating a picture into various parts of varying criticalness which is related with the picture's quality. It looks like the Fourier Transform Technique as it changes over a picture from its spatial area into recurrence space. In this procedure, for each shading constituent, the JPEG arrangement of picture makes utilization of cosine change to change over back to back pixel pieces of size 8x8 into a number of 64 cosine coefficients each. For each 8x8 piece having pixel esteem f (x, y), the coefficients f (u, v) are given as [15].

$$f(u,v) = \frac{1}{4} C(u) C(v) \left[\sum_{x=0}^{7} \sum_{y=0}^{7} f(x,y) \cos \frac{(2x+1)u\pi}{16} \cos \frac{(2x+1)v\pi}{16} \right]$$

Where,

$$C(u) = \begin{cases} \frac{1}{\sqrt{2}}, if\ u \leq 0 \\ 1, if\ u > 0 \end{cases}$$

Discrete Wavelet Transformation Technique (DWT)

Wavelets are depicted as the capacities acquired over a settled interim and have zero as a normal esteem. This change is a greatly fundamental approach to be utilized for flag examination and additionally picture handling, chiefly for multi-determination show. It might disintegrate a flag into various constituents in recurrence area. 1-D DWT portions a cover picture encourage into two noteworthy parts known as surmised segment and nitty gritty segment [16]. A 2-D DWT is utilized to portion a cover picture into primarily four sub parts: one rough segment LL (low-low) and the other three incorporate definite segments spoken to as (LH, HL, HH).

LL	HL
LH	HH

4. Audio Steganography

In Audio or sound steganography a sound record is utilized as a bearer or host document to convey mystery data or message. We can implant this mystery message in have record utilizing a key. The sound record in the wake of inserting mystery message named as stego document. This can be transmitted through a system and at the recipient the expected collector who knows key, they just concentrate mystery message from stego document as appeared in figure 3.

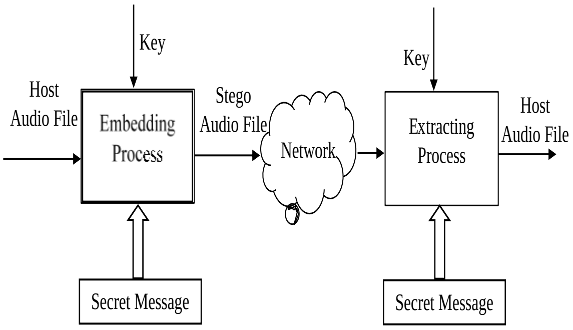

Fig. 3. Workflow model of audio steganography

4.1. PARITY CODING

One of the earlier works in sound information concealing procedure is parity or equality coding system. Rather than separating a flag into singular specimens, the equality coding strategy separates a flag into isolated locales of tests and encodes each piece from the mystery message in an example region's equality bit [17]. In the event that the equality bit of a chose area does not coordinate the mystery bit to be encoded, the procedure flips the LSB of one of the examples in the region. In this manner, the sender has to a greater degree a decision in encoding the mystery bit, and the flag can be changed in a more unpretentious manner. Figure 4, demonstrates the equality coding technique.

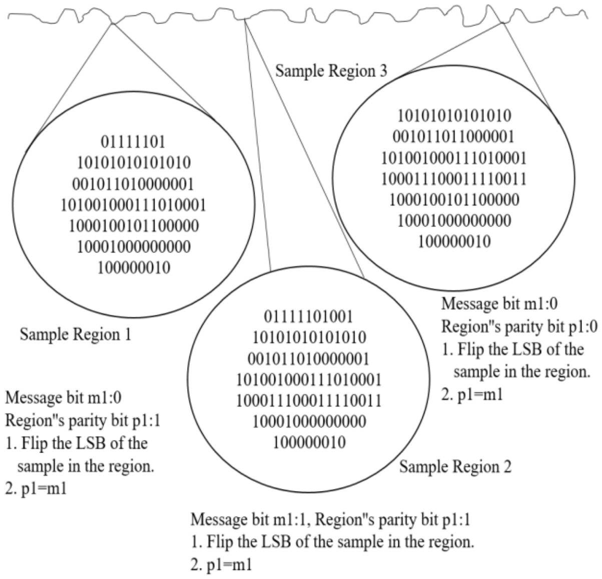

Fig. 4. Parity Coding Procedure

4.2. PHASE CODING

Phase coding addresses the impediments of the commotion prompting strategies for sound Steganography. Stage Coding works by substituting the period of an underlying sound portion with a reference stage that speaks to the data. This system depends on the way that the stage segments of sound are not as recognizable to the human ear as clamor seems to be. As opposed to presenting irritations, the strategy encodes the message bits as stage moves in the stage range of an advanced flag, accomplishing an imperceptible encoding regarding signal-to-perceived noise ratio (SPNR). Figure 5, demonstrates the phase coding technique.

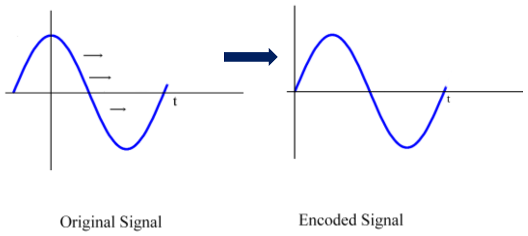

Fig. 5. Phase coding technique

4.3. SPREAD SPECTRUM

In sound steganography, the Spread Spectrum (SS) strategy endeavors to spread mystery data over the recurrence range of the sound flag utilizing a code which is autonomous of the real signal [18]. Direct-sequence and Frequency-hopping schemes are the two forms of Spread Spectrum which can be utilized as a piece of sound Steganography.

In, Direct-sequence SS endeavors to spread out the mystery message by a steady called the chip rate and after that tweaked with a pseudorandom flag and interleaved with the cover-signal.

In Frequency-hopping schemes SS, the recurrence range of sound documents is changed with the goal that it jumps quickly between frequencies.

4.4. ECHO HIDING

In echo or resound concealing, data is implanted in a sound record by bringing a reverberate into the discrete flag. As like the spread range technique, it too gives favorable circumstances in that it takes into account a high information transmission rate and gives better power when thought about than the commotion actuating strategies. In the event that just a single reverberate was delivered from the first flag, just a single piece of data could be encoded. In this way, the first flag is separated into squares prior to the encoding procedure starts. Once the encoding procedure is finished, the pieces are linked back together to make the last flag [19].

5. Video Steganography

In video steganography, mystery information is installed in cover video. A fundamental model of video steganography is appeared in Fig. 6. In this segment, some essential procedures of video steganography are talked about in a word. Least Significant Bit (LSB) strategy is one of the most straightforward and basic strategies. In this strategy, LSB of cover video is supplanted by mystery information [20]. In any case, this procedure of concealing the mystery information is very little powerful as the information may lose after some document changes [21] [22]. Another technique in light of Discrete Cosine Transform (DCT) change has been presented [23].

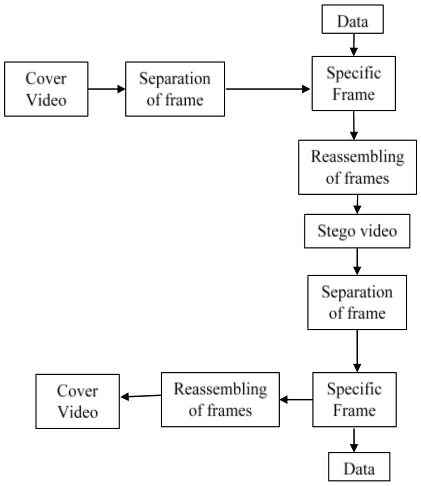

Fig. 6. Video Steganography Model

5.1. SPATIAL DOMAIN STEGANOGRAPHY TECHNIQUES

A technique in light of Least Significant Bit (LSB) was presented [24] in which mystery information is installed into the LSB of the host video outline. Execution parameters like Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) are utilized to easily measure the nature of the stego video which gives a safe system of video steganography [25]. This strategy gives list to mystery information and the record is then put in a video outline. At the less than desirable end, in spite of seeking the entire video, the mystery information can be recovered from stego video with the assistance of list. This will lessened the computational time as contrast with other existing strategies. An enhanced strategy for information stowing away in view of back spread neural system technique was proposed [26]. In this technique, neural system is utilized to perform XOR operation. Mystery information is implanted into AVI video arrange by utilizing LSB substitution system.

5.2. FREQUENCY DOMAIN STEGANOGRAPHY TECHNIQUES

Frequency Domain Steganography Techniques considered as a high payload limit video steganography technique [27]. It utilizes Lazy lifting wavelet change system for concealing the mystery data. Right off the bat wavelet is connected on the video edges and after that LSB substitution strategy is utilized to conceal information in the coefficients of video outlines. Another information concealing method in view of Discrete Cosine Transform (DCT) and the Discrete Wavelet Transform (DWT) [28]. This depends on the Markov-handle in JPEG picture steganalysis and used to recognize the concealed message in stego video [29].

6. Types of Attack

Steganography calculations give stealth and security to data. The level of stealth and security, is difficult to gauge. One approach to judge the quality of a stenographic calculation is to envision distinctive assaults and after that evaluate whether the calculation can effectively withstand them. Assaulting steganography calculations is fundamentally the same as assaulting cryptographic calculations. Here's a rundown of some conceivable assaults:

A. Record Only

The assailant approaches the record and should decide whether there is a message covered up inside.

B. Record and unique Copy

On the off chance that the assailant have a duplicate of the record with the encoded message and a duplicate of the first, pre-encoded document, at that point distinguishing the nearness of some concealed message is an inconsequential operation. The genuine question is the thing that the assailant may attempt to do with the information which may decimate shrouded data, separate the data, and supplant.

C. Various Encoded Files

The aggressor gets distinctive duplicates of the records with diverse messages. This circumstance may happen if an organization is embedding diverse following data into each document. A few aggressors may attempt to supplant the following data with their own particular adaptation of the data.

D. Pressure Attack

One of the easiest assaults is to pack the record. Pressure calculations attempt to expel the unessential data from a record, and "covered up" is frequently proportionate to "incidental".

E. Crush Everything Attack

An aggressor could just annihilate the message.

F. Arbitrary Tweaking Attacks

An aggressor could just include little, arbitrary changes to all records in the expectation of crushing whatever message might be there.

G. Reformat Attack

One conceivable assault is to change the arrangement of the record. Distinctive record positions don't store information in precisely same way of BMP, GIF, and JPEG.

H. Visual Attack

The visual assault is a stego-just assault that strips away piece of the question in way that takes into consideration a human to look for visual irregularities. The most widely recognized assault is to show the minimum huge piece of a question; Digital types of gear, for example, cameras and scanners are not flawless and frequently leave echoes at all noteworthy bits. These totally irregular commotions show the presence of a concealed message. The normal ear can get inconspicuous distinction in sound. Notwithstanding, this is a moderate and expensive assault [30].

I. Auxiliary Attack

Steganography calculations abandon a trademark structure to the information. The organization of the information record is frequently unique when data is installed. The aggressor may distinguish the nearness of a message by analysing the measurable profile of the bits. These progressions to the information document for the most part fall into effortlessly recognizable example that gives a sign of a concealed message [31].

J. Factual Attack

Factual assault is like visual assault. The way that most projects depends on the supposition that minimum critical piece of a cover record is arbitrary and thusly overwritten with a mystery message is not really genuine. The possibility of the factual assault is to think about the recurrence circulation of a potential cover record with the hypothetically expected conveyance of the cover document. In the event that the new information does not have an indistinguishable factual profile from the standard information is relied upon to have, at that point it most likely contains a shrouded message [31].

7. Encryption Tools

Some steganography programming are accessible allowed to download for your Windows PC. These have different components, similar to: stow away wrote message in pictures, conceal TXT or different sorts of records like DOCX, XLSX, ZIP, RAR and so on., upheld input cover picture groups incorporates: JPG, BMP, GIF, PNG, TIF and so on., some can shroud information in MP3, WAV, FLAC, AU, AVI and other media designs, scramble or decode information utilizing secret word, a few projects can be keep running on any stage, and that's just the beginning.

A. QuickStego

QuickStego is a free steganography programming accessible for Windows. It helps to conceal content in pictures and just clients of QuickStego can read this shrouded instant messages. Upheld input picture positions are: BMP, JPG, JPEG, and GIF, yet it spares the yield picture in BMP organize with shrouded message in it. The interface of this product is straightforward.

StegoStick

StegoStick beta is an open source steganography programming that gives a chance to shroud any sort of document in JPG, BMP, GIF, WAV, AVI, and different twofold record sorts. Four sorts of encryption systems are utilized and they are DES, Triple DES, RSA, or Default. When concealing the record in cover document it gives the "Steg" and same expansion of the cover document in the goal way. It is possible to enter solid watchword for concealing the mystery record. It has a straightforward and easy to understand interface.

Deep Sound

DeepSound is a steganography apparatus accessible free for Windows. It can shroud records of different sorts inside WAV or FLAC sound documents. It is possible to apply secret word to the scrambled records and also possible to choose the yield sound record quality too. It has a traveler like interface. It has option to join different records moreover. Snap Encode catch to spare the yield record in the coveted area.

DeEgger

DeEgger Embedder is a little and simple to utilize free programming which gives a chance to conceal delicate or mystery information into media documents. The media documents could be of any organization including JPG, PNG, MP3, and AVI and so on. It has an easy to understand interface. The host record looks like typical document and can be opened as a matter of course program yet it contains your mystery information too. You can consolidate or extricate information by utilizing it.

8. CONCLUSION

In this current time, where innovation is creating at quick pace and every day new improvements are made, security is of most extreme need. The information should be protected secure thus that it could be gotten to just by the approved organization and any unapproved client can't have any entrance of that information. Information sharing is expanding as a large number of messages and information is being transmitted on web ordinary starting with one place then onto the next. The assurance of information is prime worry of the sender. The need is that right information ought to be sent however furtively that exclusive the recipient ought to have the capacity to comprehend the message. Steganography is the foremost part utilized idea from the old circumstances. Steganography idea is the utilizations to conceal the information that can be send yet not the way that two gatherings are speaking with each other. As the need of innovation expands it turned out to be all the more difficult to ensure the information, so now steganography likewise turns out to be more advanced as contrast with the earliest strategies. One can now conceal extensive measure of information inside pictures or sound documents. Steganography utilizes the steganography algorithm apparatuses that enable a client to conceal the information inside a bearer documents and media files and afterward separate the shrouded information securely.

Acknowledgment

At first, I want to express my heartiest appreciation and love to the Almighty ALLAH for keeping me in sound and solid health. I want to express appreciation and respect to all of the teachers of the Faculty of Computer and Information Technology and stuff of Al-Madinah International University (MEDIU) for their valuable advice and productive feedback. I want to show appreciation and love to my respected parents for their faith, love and support all through my entire life. After all, I want to show appreciation and respect to all of my relatives, friends, and co-workers.

References

[1] B. Dunbar, A detailed look at Stenographic Techniques and their use in an Open-Systems Environment, 2002

[2] C. Christian, An Information - Theoretic Model for Steganography, 1998

[3] N. Johnson, Survey of Steganography Software, 2002

[4] Muhalim Mohamed Amin, Subariah Ibrahim, Mazleena Salleh, Mohd Rozi Katmin, Information Hiding Using Steganography, 2003

[5] R A Isbell, Steganography: Hidden Menace or Hidden Saviour, 2002

[6] N. Provos, Probabilistic Methods for Improving Information Hiding, 2001

[7] K. Benett, Linguistic Steganography - Survey, Analysis And Robustness Concerns For Hiding Information in Text, 2004

[8] JHP Eloff. T Mrkel and MS Olivier, An overview of image steganography, 2005

[9] Souvik Bhattacharyya, and Gautam Sanyal, Study of Secure Steganography Model, 2008

[10] S. Low, N.Maxemchuk, J.Brassil, L. O'Gorman, Document Marking and Identification Using both Line and Word Shifting, 1995

[11] L. Y. Por, T. F. Ang, and B. Delina, WhiteSteg - A New Scheme in Information Hiding Using Text Steganography, 2008

[12] Arvind Kumar, Km. Pooja, Steganography - A Data Hiding Technique, 2010.

[13] N. F. Johnson and S. Katzenbeisser, A Survey of Stenographic Techniques in Information Hiding Techniques for Steganography and Digital Watermarking, 2000

[14] Inderjeet Singh, Sunil Khullar, Dr. S. C. Laroiya, DFT Based Image Enhancement and Steganography, 2013

[15] D.R. Denslin Brabin, Dr.V.Sadasivam, QET Based Steganography Technique for JPEG Images, 2009

[16] G.Prabakaran & R.Bhavani, A Modified Secure Digital Image Steganography based on Discrete Wavelet Transform, 2012

[17] K. Gopalan, Audio Steganography Using Bit Modification, 2003

[18] Bender W, Gruhl D & Morimoto N, Techniques for Data Hiding, 1996

[19] K. Gopalan and S. Wenndt, Audio Steganography for Covert DataTransmission by Imperceptible Tone Insertion, 2004

[20] C.S. Lu, Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property, 2003

[21] J.J. Chae and B.S. Manjunath, Data hiding in Video, 1999

[22] Provos, N., Honeyman, P., Hide and Seek: An Introduction to Steganography, 2003

[23] Y. Wang, E. Izquierdo, High - Capacity Data Hiding in MPEG-2 Compressed Video, 2002

[24] Mrudul Dixit, Video Steganography, 2015.

[25] Balaji R., Secure Data Transmission Using Video Steganography, 2011

[26] Richa K., Video Steganography by LSB Technique using Neural Network, 2014

[27] Patel, K., Lazy Wavelet Transform Based Steganography in Video, 2013

[28] Qingzhong Liu, Video Steg analysis Based on the Expanded Markov and Joint Distribution on the Transform Domains Detecting MSU Stego Video, 2008

[29] Noda, H., Application of BPCS steganography to wavelet compressed video, Image Processing, 2004

[30] Arvind Kumar, Km. Pooja, Steganography - A Data Hiding Technique, 2010.

[31] Pratap Chandra Mandal, Modern Steganographic technique: A Survey, 2012.

[32] Hilles, S., & Maidanuk, V. P. (2014). Self-organization feature map based on VQ components to solve image coding problem. ARPN Journal of Engineering and Applied Sciences. Vol. 9,№ 9: 1469-1475.