ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2014

A Comparative Study on Cryptography and Steganography

R. Srinivasan[1], V. Saravanan[2], G. Selvananthi[3]

Professor and Head, Department of IT, PSV College of Engineering and Technology, Krishnagiri, Tamilnadu, India[1]

Assistant Professor, Department of IT, PSV College of Engineering and Technology, Krishnagiri, Tamilnadu, India[2]

PG Student, Department of IT, PSV College of Engineering and Technology, Krishnagiri, Tamilnadu, India[3]

ABSTRACT: The data like username, password, and others will be hacked by the hackers and they can abuse the same. This issue can be comprehended typically by utilizing encryption and decryption algorithms. Encryption is a procedure of changing over clear secret data into indiscernible structure (Cipher Text). Decryption is a methodology of changing over the mixed up cipher text into decipherable structure. Both sender of the data and the beneficiary of the data utilizes same key for encrypting and decrypting. Yet the encryption and decryption algorithms have not given 100% security. The reason is that the hackers effortlessly will discover the key by catching the packets and breaking down the jaunty text utilizing different software and fittings. So we need an alternate way like steganography for hiding sensitive information. Even though both cryptography and steganography has its own advantages and disadvantages, we can combine both the techniques together. This paper presents a comparative study of both cryptography and steganography.

KEYWORDS: Cryptography, Steganography, Encryption, Decryption, Security.

I. INTRODUCTION

System security essentially includes in keeping up system trustworthiness, keeping unapproved clients from steeling touchy data, password and so on. Substantial system are essentially assaulted by this issues, in light of the fact that they offer more powerless focuses at which gatecrashers can get access. On the off chance that the system is having numerous clients, numerous passwords and numerous systems implies the hackers can attempt it in numerous spots. By utilizing firewalls, proxies, introducing solid antivirus software we can have the capacity to lessen these issues. Additionally to conceal the touchy data from hackers two classes of procedures can be utilized, that is cryptography and steganography. This paper shows in insight about both the methods with correlation.

The hubs in a distributed system will correspond with each other, the data traded by these hubs can be effectively hacked by utilizing any one or a greater amount of the hacking instruments, for example, IP Sniffer (Build around packet sniffer), Nagios (The Open Source Network Monitoring Software), MRTG (The Open Source Traffic Monitoring Software), REMSTATS (Network observing software), Sysmon (Network checking software), Cricket (Router checking), MRTG (Traffic observing), Ntop (Traffic checking) and Kismet (Wireless examining) which is accessible in the business. These apparatuses by and large used to screen the system status yet the hackers can use to hack the data. The data like ledger subtle elements, username, password, individual points of interest and increasingly will be hacked by the hackers and they can abuse the same.

This issue can be comprehended typically by utilizing encryption and decryption algorithms (Cryptography). Encryption is a procedure of changing over clear secret data into indiscernible structure (Cipher Text). Decryption is a methodology of changing over the mixed up cipher text into decipherable structure (plain text). Both sender of the data and the beneficiary of the data utilizes same key for encrypting and decrypting. Yet the encryption and decryption algorithms have not given 100% security. The reason is that the hackers effortlessly will discover the key by catching the packets and breaking down the jaunty text utilizing different software and fittings. In view of the encryption calculation and key length the time taken for the hackers to discover the key may shift.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2014

If there should be an occurrence of customer server building design arrange, the servers validate the customers by login process. Amid the login process the customer needs to send the username and password. This username and password can be effortlessly skirted by the assaults like "SQL Injection", where the approval is not done appropriately. Additionally utilizing the infection and worm programs the hackers will gather the secret data from any hub. Indeed the IP packet following to discover the programmer or infection program engineers is an exceptionally extreme occupation today. Since the infection projects will sit in an alternate machine and do the needful. Much research has been led in the past to beat the security issues in machine systems. Numerous encryption algorithms have created and much security systems got proposed, however till today we are confronting numerous issues identified with security.

To enhance the security one can utilize an alternate technique to shroud data and to send it through system without dread called stenography. It is a craft of concealing data in multimedia components like picture, feature and liveliness and so forth. By and large, all the multimedia components are put away in the stockpiles gadgets as paired qualities. The double values can be changed to shroud secret data. Modifying few bits may not change creativity of the picture, yet in the event that the progressions are excessively high then, innovation of the picture will be ruined. So to shroud few kilo bytes of data we require few mega bytes of multimedia components. Joining both stenography and cryptography together will enhance the security drastically.

II. CRYPTOGRAPHY

Cryptography is the method of transmitting the data in a protected structure implies the plain text will be changed over into cipher text utilizing encryption and decryption techniques [1]. Just the sender and the collectors can recognize the first text. While transmitting the data the sender will send a secret key to the recipient utilizing this secret the collector can have the capacity to unscramble the first text [2].

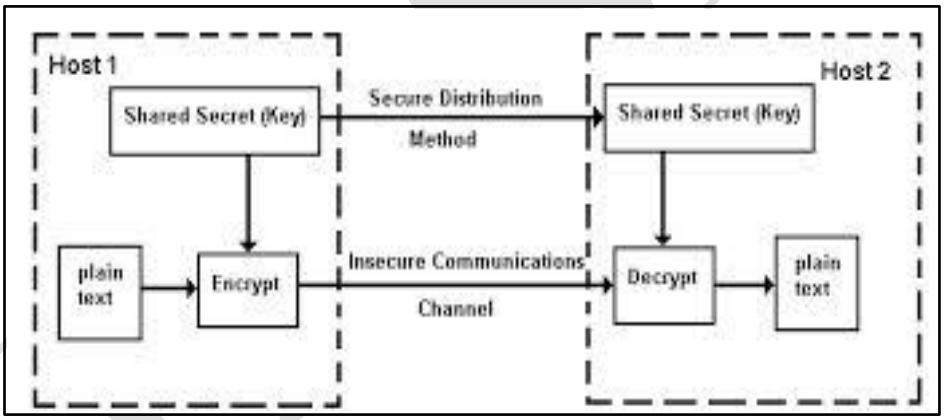

Fig. 1 Cryptography

Figure 1clarify the idea of encryption and decryption prepare by utilizing an imparted secure key idea, the Host1 is sending an encoded plain text alongside an imparted secret key before transmitting the data to the recipient the sender will send the imparted secret key to the collector then the sender will exchange the scrambled text the beneficiary will unscramble the text by utilizing the Shared secure that has been imparted by the sender at the time of correspondence [3]. Cryptography Techniques can be classified as

1. Stream cipher
2. Block Cipher

Block cipher will be having the altered length; the data can be breaks into number of blocks in a settled length. This procedure will be more helpful in transmission of vast data. For instance if M is a plaintext message then block cipher breaks M into progressive blocks M1, M2, and so on., and enciphers for every Mi with the same key K, that is EK(M)=EK(M1)EK(M2) and so on each one square is commonly a few characters long.

Example of block ciphers:

1. Play fair cipher: It is a block cipher of size 2 letters.

DOI: 10.15680/IJIRSET.2014.0312044

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2014

2. HILL cipher: It is a block cipher of size D letters.
3. DES cipher: It is a block cipher of size 64 bits.
4. Electronic code book (ECB).

Advantages of Block Cipher

1. It is sort of quicker than stream cipher each one time n characters executed.
2. Transmission slips in one cipher text square have no influence on different blocks.

Disadvantages of Block Cipher

1. Identical blocks of plaintext produce indistinguishable blocks of cipher text.
2. Easy to embed or erase blocks.

Stream Cipher

Stream cipher will be having the plaintext digits, and every digit is encoded with the comparing keystream. It is breaks the message M into progressive characters or bits M1, M2, and so forth and enciphers every Mi with the it component Ki of a key stream K=K1K2 and so on. That is EK(M)=EK1(M1)EK2(M2) and so on.

Example of Stream Cipher

1. One time bits and Running key ciphers are non occasional and Vigenere cipher is intermittent on the grounds that plain text scorch are enciphered one by one and Adjacent roast are encipher with an alternate block of the key.
2. Auto key cipher: An Auto key cipher is sample on synchronous toward oneself such that the Key is gotten from the message it encipher in vigeneres first cipher the key is framed by affixing the plain text M=m1m2 and so forth to a "preparing key" character ki ,the i-th key Character (i>1)) begins with k1, next key Ki=mi-1 or Ci-1.
3. Cipher input (CFB): It is an alternate case on self- synchronous such that plain text is enciphered in little units (littler than block size).

A stream cipher is intermittent if the key stream rehashes after characters for some altered else it is no occasional.

Advantages of Stream Cipher

1. Stream cipher that just encryption and decryption data one bit at once are truly suitable for hard product execution.
2. Easy to examine scientifically.

Drawbacks of Stream Cipher

1. Transmission slip in one cipher text square have influence on other block such that if a bit lost or a changed amid transmission the mistake influence then character and cipher resynchronise itself after n right cipher text singe.
2. It is slower than square however we can make it all the more quickly by actualized in unique reason equipment fit for encryption a few million bits for second.

Limitation of Cryptography Technique

1. Key Distribution: As the keys at both the side ought to be same, it needs to be traded first. So if the media for trading the key is traded off, it turns into a debacle.

DOI: 10.15680/IJIRSET.2014.0312044

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2014

2. Traded off KDC: In the event that we are utilizing a key dispersion focus (KDC) to trade the keys and the KDC itself is bargained it additionally turns into a limit.
3. Arbitrary Number Generation: We utilize arbitrary numbers for the era of cipher text in the change capacity. One issue with this irregular number generator is that the numbers produced won't be consummately arbitrary. So there is plausibility that it can be speculated.
4. Arrangement of Encryption Function: On the off chance that the encryption capacity is not appropriately set it can prompt spillage of data.
5. Data Recovery Agent: In windows based encryption is predominantly focused around the client password, the overseer will be having the rights to recuperation the password if there should be an occurrence of any data missing.
6. Utilizing Same Password: Utilizing the effectively speculated password and recording the password on the notepad, or utilizing the same password for some pages will prompt powerless.
7. Key Management: In an association the individuals needs to peruse a specific scrambled document implies they have to memories the key, this can be feasible for having one or two people groups however for a substantial association it is impractical.

III. FUNDAMENTALS OF IMAGES

As discussed in [4], a computerized picture is a numeric representation of a two-dimensional picture. Contingent upon whether the picture determination is altered, it might be have vector or raster sort. Without anyone else's input, the expression "advanced picture" normally alludes to raster pictures or bitmapped pictures. Raster pictures have a limited set of advanced qualities, called picture components or pixels. The computerized picture contains a settled number of columns and sections of pixels. Pixels are the littlest individual component in a picture, holding quantized values that speak to the splendor of a given colour at any particular point.
Normally, the pixels are put away in machine memory as an issue picture or raster outline, two-dimensional cluster of little whole numbers. These qualities are regularly transmitted or put away in a layered structure. Raster pictures can be made by an assortment of data gadgets and methods, for example, advanced cams, scanners, direction measuring machines, seismographic profiling, airborne radar, and then some. They can likewise be synthesized from arbitrary non-picture data, for example, scientific capacities or three-dimensional geometric models; the recent being a real sub-territory of machine representation. The field of computerized picture transforming is the investigation of algorithms for their change.

Digital Image File Formats

Most clients come into contact with raster pictures through advanced cams, which utilize any of a few picture file forms. Some advanced cams offer access to just about all the data caught by the cam, utilizing a crude picture group. The Universal Photographic Imaging Guidelines (UPDIG) recommends these arrangements be utilized when conceivable since crude files deliver the best quality pictures. These file configurations permit the picture taker and the transforming operators the best level of control and exactness for yield. Their utilization is inhibited by the pervasiveness of restrictive data (prized formulas) for some cam producers; however there have been activities, for example, Open RAW to impact makers to discharge these records openly. An option may be Digital Negative (DNG), a restrictive Adobe item portrayed as "people in general, archival organization for advanced cam crude data". In spite of the fact that this organization is not yet generally acknowledged, help for the item is developing, and progressively proficient documenters and progressives, working for respectable associations, differently propose or prescribe DNG for archival purposes.

By and large talking, in raster pictures, Image file size is emphatically connected to the quantity of pixels in a picture and the shade depth, or bits every pixel, of the picture. Pictures can be layered in different ways, in any case. Layering uses a calculation that stores a careful representation or an estimate of the first picture in a littler number of bytes that can be stretched over to its uncompressed structure with a relating decompression calculation. Considering distinctive compressions, it is normal for two pictures of the same number of pixels and shade depth to have an altogether different layered file size. Considering precisely the same layering, number of pixels, and shade depth for two pictures,

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2014

diverse graphical intricacy of the first pictures might likewise bring about altogether different file sizes after squeezing because of the way of clamping algorithms. With some pressure configurations, pictures that are less unpredictable may bring about littler packed file sizes. This trademark some of the time brings about a littler file size for a few lossless organizations than lossy arrangements. For instance, graphically basic pictures (i.e. pictures with expansive persistent districts like line craftsmanship or activity groupings) may be losslessly packed into a GIF or PNG configuration and bring about a littler file size than a lossy JPEG design.

Picture File Compression

As discussed in [5], there are two sorts of picture file clamping algorithms: lossless and lossy. Lossless pressure algorithms decrease file size while saving an immaculate duplicate of the first uncompressed picture. Lossless packing for the most part, yet not generally, brings about bigger files than lossy layering. Lossless squeezing ought to be utilized to abstain from amassing phases of re-layering when altering pictures. Lossy squeezing algorithms protect a representation of the first uncompressed picture that may have all the earmarks of being an immaculate duplicate, yet it is not an impeccable duplicate. Frequently lossy packing has the capacity attain littler file sizes than lossless layering. Most lossy layering algorithms take into account variable clamping that exchanges picture quality for file size.

JPEG/JFIF

JPEG (Joint Photographic Experts Group) is a lossy squeezing technique; JPEG-layered pictures are generally put away in the JFIF (JPEG File Interchange Format) file position. The JPEG/JFIF filename expansion is JPG or JPEG. About every computerized cam can spare pictures in the JPEG/JFIF design, which underpins 8-bit grayscale pictures and 24-bit shade pictures (8 bits each for red, green, and blue). JPEG applies lossy layering to pictures, which can bring about a noteworthy diminishment of the file size. Applications can focus the level of packing to apply, and the measure of layering influences the visual nature of the result. At the point when not very extraordinary, the layering does not discernibly influence or degrade the picture's quality, however JPEG files endure generational corruption when more than once altered and spared. (JPEG additionally gives lossless picture stockpiling, yet the lossless form is not generally backed.)

JPEG 2000

JPEG 2000 is a clamping standard empowering both lossless and lossy stockpiling. The packing routines utilized are not quite the same as the ones in standard JFIF/JPEG; they enhance quality and clamping degrees, additionally require more computational force to process. JPEG 2000 additionally includes emphasizes that are absent in JPEG. It is not about as basic as JPEG, yet it is utilized at present as a part of expert film altering and dissemination (some computerized films, for instance, use JPEG 2000 for individual motion picture outlines).

Exif

The Exif (Exchangeable picture file organization) configuration is a file standard like the JFIF group with TIFF augmentations; it is incorporated in the JPEG-composing software utilized as a part of generally cams. Its intention is to record and to institutionalize the trading of pictures with picture metadata between computerized cams and altering and review software. The metadata are recorded for individual pictures and incorporate such things as cam settings, time and date, screen speed, introduction, picture size, packing, name of cam, shade data. At the point when pictures are seen or altered by picture altering software, the majority of this picture data can be shown. The real Exif metadata in that capacity may be conveyed inside diverse host groups, e.g. TIFF, JFIF (JPEG) or PNG. IFF-META is an alternate case.

DOI: 10.15680/IJIRSET.2014.0312044

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2014

TIFF

The TIFF (Tagged Image File Format) arrangement is an adaptable configuration that typically spares 8 bits or 16 bits every shade (red, green, blue) for 24-bit and 48-bit sums, separately, generally utilizing either the TIFF or TIF filename expansion. The labelled structure was intended to be effortlessly extendible, and numerous merchants have presented restrictive unique reason labels with the come about that nobody peruses handles each kind of TIFF file [5]. Some computerized cams can spare pictures in TIFF configuration, utilizing the LZW clamping calculation for lossless stockpiling. TIFF picture arrangement is not broadly backed by web programs. TIFF remains generally acknowledged as an issue file standard in the printing business. TIFF can deal with gadget particular shade spaces, for example, the CMYK characterized by a specific set of printing press inks. OCR (Optical Character Recognition) software bundles generally generate some manifestation of TIFF picture (frequently monochromatic) for examined text pages.

Crude

Crude alludes to crude picture organizes that are accessible on some computerized cams, instead of to a particular organization. These arrangements typically utilize a lossless or almost lossless squeezing, and produce file sizes littler than the TIFF designs. Despite the fact that there is a standard crude picture form, (ISO 12234-2, TIFF/EP), the crude configurations utilized by most cams are not institutionalized or archived, and contrast among cam makers. Most cam makers have their software for interpreting or creating their crude file position, however there are additionally a lot of people outsider crude file converter applications accessible that acknowledge crude files from most advanced cams. Some realistic projects and picture editors may not acknowledge some or all crude file configurations and some more seasoned ones have been viably stranded as of now.
The extent that camcorders are concerned, ARRI's Arriflex D-20 and D-21 cams give crude 3k-determination sensor data with Bayer design as still pictures (one every edge) in an exclusive arrangement (.ari file expansion). Red Digital Cinema Camera Company, with its Mysterium sensor group of still and camcorders, uses its exclusive crude configuration called REDCODE (.R3d expansion), which stores still and additionally audio and video data in one lossy-layered file.

GIF

GIF (Graphics Interchange Format) is restricted to a 8-bit palette, or 256 shades. This makes the GIF design suitable for putting away illustrations with generally few colors, for example, straightforward graphs, shapes, logos and toon style pictures. The GIF arrangement helps activity is still generally used to give picture liveliness impacts. Its LZW lossless squeezing is more compelling when extensive territories have a solitary colour, and less viable for photographic or dithered pictures.

IV. FUNDAMENTALS OF DIGITAL VIDEOS

Digital feature embodies an arrangement of orthogonal bitmap advanced pictures showed in quick progression at a consistent rate [7]. In the context of feature these pictures are called casings. We quantify the rate at which casings are shown in edges every second (FPS). Since each casing is an orthogonal bitmap advanced picture it includes a raster of pixels. On the off chance that it has a width of W pixels and a tallness of H pixels we say that the casing size is WxH. Pixels have one and only property, their shade. The shade of a pixel is spoken to by a settled number of bits. The more bits the more inconspicuous varieties of colours can be recreated. This is known as the colour depth (CD) of the feature. A case feature can have a span (T) of 1 hour (3600sec), an edge size of 640x480 (WxH) at a shade depth of 24bits and a casing rate of 25fps. This illustration feature has the accompanying properties:
Pixels per frame = 640 * 480 = 307,200
Bits per frame = 307,200 * 24 = 7,372,800 = 7.37Mbits
Bit rate (BR) = 7.37 * 25 = 184.25Mbits/sec
Video size (VS) = 184Mbits/sec * 3600sec = 662,400Mbits = 82,800Mbytes = 82.8Gbytes
The most important properties are bit rate and video size. The formulas relating those two with all other properties are:

DOI: 10.15680/IJIRSET.2014.0312044

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2014

BR = W * H * CD * FPS
VS = BR * T = W * H * CD * FPS * T
(units are: BR in bit/s, W and H in pixels, CD in bits, VS in bits, T in seconds)
While some secondary formulas are:
Pixels_Per_Frame = W * H
Pixels_Per_Second = W * H * FPS
Bits_Per_Frame = W * H * CD

Regarding Interlacing

In interweaved feature each one edge is made out of two parts of a picture. The principal half contains just the odd-numbered lines of a full edge. The second half contains just the even-numbered lines. Those parts are alluded to independently as fields. Two successive fields create a full edge. In the event that an interweaved feature has an edge rate of 15 edges every second the field rate is 30 fields every second. All the properties and recipes examined here apply similarly to entwined feature yet one ought to be mindful so as not to befuddle the fields every inferior with the edges every menial.

V. STEGANOGRAPHY

As said in [9], above the process of hiding information inside another media is called stegnography. The media with secret information is called stego media and without hidden information is called cover media. Steganalysis is a process of extracting information from the stego media. Steganalysis is just opposite to stegnography. Any image is made up of pixels. Each pixel represents a color value and depends upon the image the pixel size will be from 1 bit to 4 bytes. These pixels will be stored in a computer memory in binary form. Let us consider an image with pixel size 2 bytes for discussion. The pixel with 2 byte size can able to represent 216 different colors, range from 0000000000000000 to 1111111111111111. Normally for human eyes the color 1111000011110000* and 1111000011110001* will look like similar, since the difference is too low. Which means that the change in least significant bit (*LSB) may not be noticed by human eyes. If we alter 1111000011110000 as 0111000011110000, then the color of a pixel will change to another color. That is the change in the most significant bit (MSB), will change the color dramatically. This can be easily identified by everyone. So it is clear that the secret information has to be stored in the LSB and not in MSB of the cover image to reduce the detectable distortion. The performance of a stegnography can be measured by three factors. They are security, capacity and detectable distortion (DD). The security must be high, so that the active attacks and passive attacks should not succeed in finding secret information.

Classification of steganography categories

Steganography is ordered into 3 classifications,

1. Pure Steganography: In this strategy there is no stegno key, just focused around the supposition and other gathering is not mindful of the correspondence.
2. Secret key steganography: In this strategy the steganography key is traded before the correspondence and this is most suspectible to interference.
3. Public key steganography: In this strategy open key and the private key is utilized for correspondence

Classification of Steganography strategies

Steganography strategies are characterized into six classes they are

1. Substitution strategies substitute repetitive parts of a spread with a secret message (spatial space).
2. Transform space systems insert secret data in a change space of the signal (frequency area).
3. Statistical strategies encode data by changing a few factual properties of a spread and utilization speculation testing in the extraction process.
4. Distortion procedures store data by sign mutilation and measure the deviation from the first cover in the interpreting step.
5. Cover era system will cover the data for secret correspondence.

DOI: 10.15680/IJIRSET.2014.0312044

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2014

Advantages of Steganograph

As discussed in [8], the following are the few advantages of using steganography

- As mentioned in table 1 secret information can be shuffled anyway we like, so the secret information cannot be identified by the hackers.
- Coding secret message in digital images is one of the main advantages in steganography.
- Steganography does not alter the structure of the original message.
- Steganography will provide secret way of communication of the original message.
- Steganography is used to hide the secret message in audio, video and in text messages.
- Steganography is used to hide one file into another file.
- The main aim of steganograhy is to improve security, capacity with minimum distortion.

Cryptography	Steganography
Known message passing is done	Unknown message passing is done
Encryption prevents an unauthorized party from recovering the contents from communication	Steganography prevents discovery of the very existence of communication
Common technology is used	Little known technology is used
Most of the algorithm are known	Technology still being developed for certain format
Strong current algorithm are resistant to attack and larger expensive power is needed to crack those algorithms.	Once detected, message is known
Cryptography alter the structure of the secret message	Steganography does not alter the structure of the secret message

Table 1. Comparison of Cryptography and Steganography [8]

VI. CONCLUSION

In this paper we have discussed a lot about various image and video formats with fundamentals. Also we have discussed about cryptography and steganograph with comparison. As everyone knows that security issue in a challenging issue today in every computer networks. To solve this issue enhancement in cryptography or steganography is very essential. Also enhancing cryptography or steganography alone is not sufficient. Hence both cryptography and steganography has to be enhanced for the future security needs and integrated with each other for better security.

REFERENCES

[1] Http://searchsoftwarequality.techtarget.com/definition/cryptography
[2] Www.netwidget.net
[3] Uday Sabri Abdul Razak, Ameer Al-Swidi, "An advantages and Dis Advantages of Block and Stream Cipher", Basic Education College Magazine For Educational and Humanities Sciences (294-297), Volume 1, No.2, 2010
[4] Http://en.wikipedia.org/wiki/Digital_image
[5] Http://en.wikipedia.org/wiki/Image_file_formats
[6] Gurmeet Kaur, Aarti Kochhar,"Transform Domain Analysis of Image Steganography", International Journal for Science and Emerging Technologies with Latest Trends (29-37), Vol. 6 Issue 1, 2013
[7] Http://en.wikipedia.org/wiki/Digital_video
[8] A. Joseph Raphael, Dr. V. Sundaram, "Cryptography and Steganography", International Journal of Computer Technology and Applications (626-630), Vol. 2 Issue 3, 2011
V. Saravanan and A. Neeraja, "Security Issues in Computer Networks and Stegnography", in Proceedings of 7th International Conference on Intelligent Systems and Control (ISCO 2013), pp. 363-366, Coimbatore, Tamilnadu, India, January 2013