Video Steganography Using Encrypted Payload for Satellite Communication

Swadhin Thakkar[1] **, Kaustubh Shivdikar**[2] **, Chirag Warty**[3]
Research Fellow[1]**, Solutions Architect**[2]**, Chief Solutions Architect**[3]
Quanical Innovation Lab, Mumbai, India[123]
thakkar.swadhin.a@ieee.org [1]**, kaustubh.c.shivdikar@ieee.org** [2]**, chiragwarty@ieee.org** [3]

Abstract—**In November 2014, a massive cyber-attack on a major company leaked sensitive data including thousands of personal records. Despite the fact that a lot of research and development has gone in the past decade to develop robust encryption algorithms, hackers have managed to break them. Effective information security is an important aspect and cannot be undermined in today's times. When an adversary intercepts encrypted data, it can be known that a secret message was sent. This can raise alarms and invite attacks. Moreover, many times it is important to communicate secretly without drawing any attention and not raise suspicion even if the message is intercepted. We feel that the key to heightened security is to not only encrypt the data but to hide the fact that secret message is being sent. This is implemented by steganography. Steganography is the science of concealing information (secret message) in an apparently innocuous media file (image, audio, video). We use an algorithm to hide the message inside the carrier (cover) media. Although steganography facilitates covert communication, it suffers from attacks like detection, modification, extraction and destruction. In this paper, we present a powerful combination of steganography and cryptography - a novel method to realize a highly secured level of communication. The proposed system encrypts the secret message via secure encryption algorithms and spreads it out over a broad bandwidth using spread spectrum technique. Then, we embed it into the cover media without affecting the perceptual fidelity as the amount of encoded information is below the threshold of perception and is regarded as noise. The original video is available at the receiver for successful retrieval of the secret message. This paper achieves additional security layer of data authentication and integrity check by adding a Hash-based Message Authentication Code (HMAC) module to the message. Further, we analyze the performance of the proposed technique towards different detection, modification and destruction attacks. The proposed blend of techniques showcases a higher immunity to these attacks while maintaining private, confidential communication. The proposed system is briefly discussed in the context of satellite communication.**

Keywords - Video Steganography, RSA Encryption, Spread Spectrum, HMAC, Bit Substitution, SSIM, Satellite Communication, Inter-Satellite Link (ISL)

TABLE OF CONTENTS

1. INTRODUCTION

Cryptography is the practice and study of techniques for secure communication in the presence of third parties called adversaries [1]. More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages [2]. The growth of cryptographic technology has raised some legal issues in the information age. Cryptography's potential for use as a tool for espionage and sedition has led many governments to classify it as a weapon and to limit or even prohibit its utilization and export [3]. In some jurisdictions where the use of cryptography is legal, laws permit investigators to compel the disclosure of encryption keys for documents relevant to an investigation [4] [5]. Therefore, it becomes compelling to make use of other techniques to carry out secret communication without inviting attention.

Present day requirements of security systems are confidentiality, authenticity, integrity, and non-repudiation. The need to have total secrecy in an open-systems environment is the main idea behind steganography. Steganography is derived from the Greek words 'stegos' meaning 'cover' and 'grafia' meaning 'writing.' Throughout history, steganography has been used to secretly communicate information between people. Few examples of steganography from the past are discussed from [6].In ancient Greece, messengers used to shave their head. Then a message would be written on their heads and hair was allowed to grow back. He was sent to deliver the message only after the hair grew back. The recipient would shave off the messenger's hair and receive the message. Another method used in Greece was by peeling the wax off a tablet which was covered in wax. A message would be written underneath the wax, and then wax was reapplied. The recipient of the message would simply remove the wax from the tablet to view the message. During World War 2, an invisible ink was used to write messages on pieces of paper. Liquids such as milk and vinegar were used. It appeared to the average person as just being blank pieces of paper. However, when these substances are heated, they darken and become visible to the human eye.

While cryptography keeps the content of the message secret, steganography aims at hiding the existence of messages. Digital steganography is currently an active research area and has applications in hidden communications, image authentication and copyright protection. Information concealment can be used for secure communication. Hiding messages inside other seemingly harmless messages in a way that does not allow any enemy even to detect that there is a second message present is the essence of steganography. This feature enables it to have true confidentiality and secrecy. Steganographic techniques are also crucial to safety and privacy on the internet, as most of the data is routed via public.

978-1-5090-1613-6/17/31.00 ©2017 IEEE

Steganography replaces redundant data in the cover media with the secret information to be sent. The key idea is inserting the information inside a cover media as noise. This noise is similar to the one native to the communication of data across noisy channels. This noise is regarded as one generated as a consequence of the channel and hence is not perceptible to humans or computer analysis, if it is kept at low levels [7]. Without real awareness of the presence of secret information or access to the original media, it is tough for a party to know whether the information is embedded. Moreover, even if they have doubt that secret information is being sent, it is tough to find out what it is, when powerful steganographic techniques are used. The requirement is that the carrier media must contain a sufficient amount of redundant data or noise to accommodate a secret message. This requirement limits the types of data that we can use in steganography [8]. The cover media can be text, image, audio or video. Steganography can be used in different types of data formats in today's world of digital communication. The popular data formats for cover media are .bmp, .doc, .gif, .jpeg, .mp3, .txt and .wav. The secret message is a stream of information which is in the form of bits.

Most of the current steganographic methods rely on two parameters - the secret key and the strength of the steganographic algorithm. However, they either do not address the issue of encryption of the payload before embedding or just use one or more of the conventional cipher algorithms. Hence, Westfeld et. al. concluded their CRYSTAL project with an important observation that "Crypto-Stego interaction is not very well researched yet" [9]. Some authors have discussed encryption of the payload before embedding [10].

Steganalysis is the study of detecting messages hidden using steganography; this is analogous to cryptanalysis applied to cryptography. Steganalysis involves the practice of attacking steganographic methods by detection, destruction, extraction or modification of embedded data [8]. The strength of embedding algorithms depends on how immune is it to the various attacks carried out. Cryptanalysis is considered successful when the attacker retrieves information successfully from the message. Whereas steganography involves an additional criterion the attacker should not know about the presence of a hidden message. Knowing the fact that there is information hidden in the cover destroys the purpose of steganography. To be effective, the embedded data should be [11]:

(1) Unobtrusive / Perceptually invisible - Its presence should not interfere significantly with characteristics of the media.

(2) Robust - It should be difficult to remove and retrieve it. If only partial knowledge is available (for example known cover or known stego), then attempts to delete the message, should result in severe degradation of the cover media. The stego file should be immune to:
a. Common signal processing techniques like digital-to-analog and analog-to-digital conversion, resampling, requantization, and common signal enhancements like image contrast and color, or audio bass and treble change. It should be possible to retrieve the message even if some level of compression is applied.
b. Common geometric distortions like rotation, translation, cropping and scaling.

(3) Universal - The data should be compatible with all kinds of multimedia cover messages.

(4) Unambiguous Retrieval - The secret data should be accurately retrieved at the receiver.

(5) Authentication - The receiver should be able to confirm the validity and integrity of the message. The message should be distinctly degraded in the event of an attack.

Neither Steganography nor Cryptography can be thought of as the ultimate answer to open systems privacy, but using both technologies together can provide very high levels of privacy for anyone. Both Steganography and Cryptography are excellent means for secure communication, but neither technology alone is perfect, and both can be broken. Therefore, experts would suggest using both to add multiple layers of security [8].

Contribution - In this paper, we use a combo of cryptography and steganography. A strong encryption algorithm combined with clever steganography techniques can help achieve a highly secured level of communication. This fusion helps overcome disadvantages of both practices - disguises the otherwise obviously encrypted data and encrypts the hidden information to render extraction futile.

The paper is organized into following sections. Section 2 documents previous work. Section 3 enlists the various parameters that govern a steganography system. Section 4 discusses the embedding and extraction process in the proposed system. It also explains and evaluates the various algorithms used. Section 5 describes the application in Inter-Satellite Links (ISL). Conclusion is described in section 6.

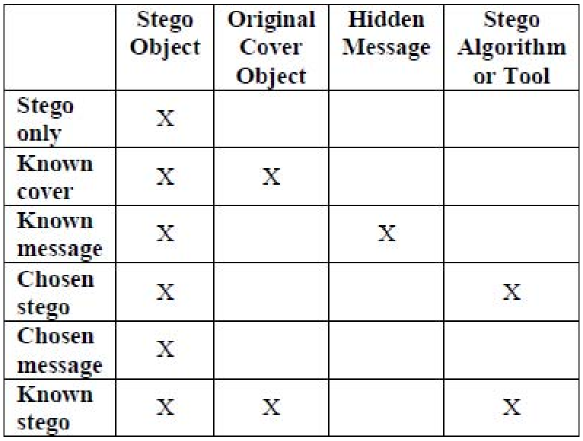
2. Previous Work

There have been various implementations of steganography and steganalysis. Some of these also employ cryptography. [12] Embeds the cipher in the image in an encrypted form using a reference database instead of direct bit variations. Asymmetric key cryptography is implemented using Data Encryption Standard (DES) algorithm. The cipher sequence can be decoded without the original image, and only the edited image will be transmitted to the receiver.

This technique [13] uses least significant bit (LSB) steganography as the basis and randomly disperses the secret message over the full picture to make sure that the secret message cannot be recovered easily from the picture. Detailed visual and statistical analysis of the algorithm reveals that it yields satisfactory results. The LSB substitution also uses plane cycling to distribute bits in the red, blue and green (RGB) planes randomly. A steganalysis method [14] is introduced to detect the existence of hidden message that is randomly embedded in LSB and the second significant bits (second-LSBs) of image pixels. It is proposed based on investigating the statistical characters of image data in LSB and the second significant bits with hidden message. The application discussed in this paper [15] ranks images in a users library based on their suitability as cover objects for some data. By matching data to a picture, there is less chance of an attacker being able to use steganalysis to recover the data. Before hiding the data in a picture, the application first encrypts it. [16] Discusses the concept of random pixel embedding instead of sequential embedding. This technique is a security feature added to the usual LSB manipulation of the pixel. [17] mentions about the upper bound on the number of bits that can be hidden in an image without causing major statistical changes. The importance of using encrypted messages is also mentioned.

The technique [6] embeds the hidden information in the spatial domain of the cover image and can verify if the attacker has tried to edit, erase or forge the secret information in the stego-image. [18] have presented a method of embedding information within digital image via a combination of techniques like spread spectrum, error control coding, and image processing. The secret information is embedded within the noise, which is then added to the digital image. [19] have proposed to identify the existence of hidden message and locate the position of the hidden information in the cover image. [20] have suggested a steganalysis of a block Discrete Cosine Transform (DCT) image steganography. Here information is hidden in each of the 8 x 8 DCT blocks. Because of the block structure of this technique, pairs of neighboring pixels within a block have different statistics from those of two 8 x 8 blocks. [21] have mentioned about the use of gray level modification of an image to embed binary data stream into the cover image. First, specific pixels are transformed, and then the binary stream is integrated into the picture. This algorithm allows secret communication. The information is hidden and recovered within the spatial domain of the image. This technique has low computational complexity and high information hiding capacity. [22] Uses a technique to encrypt the secret message and then embeds into an animation. It explains the use of error control coding and ASCII text embedding into frames of animation to propose a robust steganographic algorithm.

Steganalysis attacks can be classified in different ways. Wayner [23] divides common attack methods by functional properties; attacks fall into visual or aural, structural and statistical. Figure 1 shows six categories of detection techniques available for steganalysis [8]. It demonstrates that different attacks are possible when the attacker has access to various types of information.



	Stego Object	Original Cover Object	Hidden Message	Stego Algorithm or Tool
Stego only	X			
Known cover	X	X		
Known message	X		X	
Chosen stego	X			X
Chosen message	X			
Known stego	X	X		X

Figure 1. **Six types of detection attacks**

[11] Proposes a spread spectrum technique where data is embedded into the perceptually insignificant portions of the image. The DCT of the cover image is taken, and the information is hidden in the entire frequency spectrum. It has been noted that the frequency domain methods are more robust than the spatial domain techniques. The original image is present at the receiver for successful retrieval of the secret message. [7] Uses Spread Spectrum Image Steganography (SSIS) by spreading the classified information with a wideband signal generated with a pseudorandom sequence. The information is encrypted before being spread out. It uses interleaving to not only correct for burst errors but provides an additional level of security. It also mentions that LSB methods are vulnerable to extraction by unauthorized parties. [24] Mentions about watermarking of video via a combination of spread spectrum and modulation. Redundancy is added to the secret message which is then modulated with a pseudorandom number to embed the watermark. Because of the properties of the pseudo-noise signal, it becomes difficult for attacks to detect, locate and modify data.

3. System Parameters

There are few terms which need to be understood in the context of steganography. These elements form the building blocks of a steganography system. Figure 2 shows a typical model of steganography.

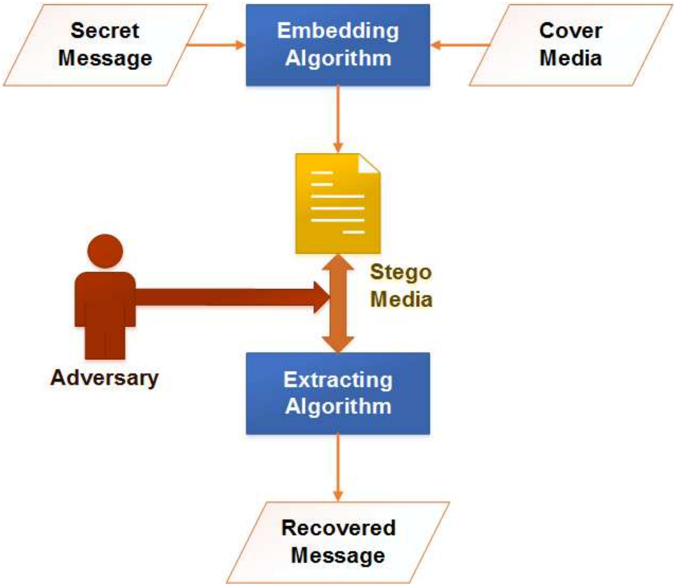


Figure 2. **Steganography Model**

Definitions:

(1) Hidden message - This is the secret data which needs to be communicated over a public channel. It can be a text, image, audio or video.

(2) Cover Media - The carrier into which the secret information is hidden. The message should be embedded in the redundant regions of the cover media. It should be done in such a way that there are no major alterations in the statistical properties of the cover.

(3) Embedding Algorithm - It is defined as the technique with which the message is embedded into the cover media. The aim of the algorithm is to not only embed the information efficiently but also not affect the quality of the cover media. For example, the visual quality of an image.

(4) Stego Media - It is the synthesized image obtained by the combination of the payload and cover media after the application of the algorithm. The stego media should be statistically similar to the cover media.

(5) Adversary - The attacker or hacker who is interested in and intends to extract the hidden information from the stego media in the communication channel.

(6) Perceptibility - It describes the ability to detect the pres-

ence of hidden information in a stego media. For example, visual perception in an image. It is dependent on the nature and complexity of embedding algorithm.

(7) Robustness - It defines how immune the payload is in the event of attacks like modification and destruction on the stego media. A robust algorithm makes it difficult for an attacker even to detect the hidden message.

(8) Security - It the level of secrecy in the process. Factors like confidentiality, authenticity and data integrity of the hidden message are taken into account. The ability of the receiver to verify error-free delivery of message corresponds to a high level of security.

Error Analysis:

(1) Mean Square Error (MSE) - It is defined as the square of the error between the cover and the stego. The distortion in the stego can be measured using MSE. The cover image is represented as 'cov' and stego image as 'steg' in the given equation.

$$MSE = \frac{\Sigma_{i=1}^{M}\Sigma_{j=1}^{N}(cov(i,j) - steg(i,j))^2}{M * N} \tag{1}$$

where M * N is the image size.

(2) Peak Signal to Noise Ratio (PSNR) - It is the ratio of the maximum signal to noise in the stego image.

$$PSNR = 20 * \log_{10} \frac{255}{\sqrt{MSE}} \tag{2}$$

(3) Bit Error Rate (BER) - The error while retrieving hidden information from a communication channel.

$$BER = \frac{1}{\mid image^{cov} \mid} \Sigma^{allpixels} \mid image^{cov} - image^{steg} \mid \tag{3}$$

(4) % BER - It is BER expressed in percentage.

$$\%BER = BER * 100 \tag{4}$$

(5) Structural Symmerty (SSIM) - It is the measurement or prediction of image quality based on an initial uncompressed or distortion-free image as reference. It is a full reference metric. SSIM is used for measuring the similarity between two images [25].

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \tag{5}$$

where μ_x is average of x, μ_y is average of y, σ_x^2 is variance of x, σ_y^2 is variance of y, σ_{xy} is covariance of x and y, k_1=0.01, k_2=0.03, L is dynamic range i.e. $2^{bitsperpixel}$-1, c_1 = (k_1 L)^2, c_2 = (k_2 L)^2.

4. System Model

Every steganographic system discussed consists of two techniques - the embedding and extraction process. The embedding process accepts three inputs - the secret message, the algorithm that defines the processes and the cover object. The output of the embedding process is called the stego object. When the stego object is presented as an input to the receiver, it produces the secret message with the help of extraction algorithm [26].

The Prisoner's problem is a common example used to explain the scenario for secure communication. The 'Warden' in this example is the communication channel between 'Alice' and 'Bob'. Warden is the entity which can compromise the communication between Alice and Bob. There are three types of Wardens - passive, active and malicious. Passive Warden only checks for the presence of secret messages and is not allowed to modify it. Active Warden may intentionally alter the message to destroy it when hidden information is detected. A Malicious Warden may impersonate and try various methods to extract the embedded information [27]. The proposed method suggests ways to counter all the three types of wardens - passive, active and malicious.

There are two elements involved in making a robust stego media - the message structure and the insertion strategy. For the stego media to be secure, these two elements must be designed correctly [11]. The proposed method describes the various algorithms for both of these elements. A flow chart of the method is shown in Figure 3.

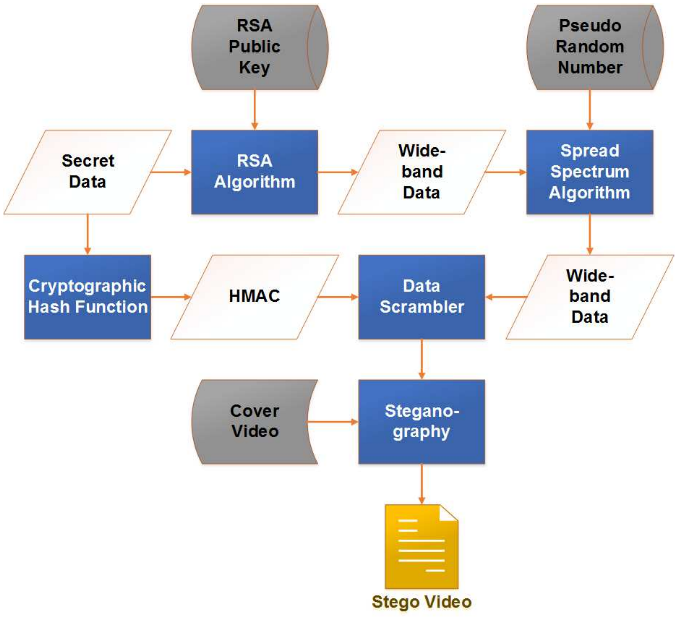


Figure 3. Proposed Method

(A) Message Structure

RSA (Rivest Shamir Adleman) Encryption:

Encrypting the data before embedding provides in-depth security. This makes attacker's task more difficult if the goal is to extract and read the secret data. The statistical properties of meaningful data can be known. However, the statistical properties of the data post-encryption may not possess similar patterns.

The payload in the proposed system is encrypted via the RSA algorithm [28]. There are two advantages in doing so. First, by using a public key the need for a shared private key between the sender and recipient is discarded. Shared keys are not practical because they require a secure way of distributing the key to parties who may want to communicate. This means sharing the key via a communication channel which is subject to detection, modification, destruction and extraction. A public key can be distributed easily by giving it to the intended parties. There is no risk even if a public key is leaked. Second, the RSA algorithm is widely known and considerably secure if large prime numbers are used to generate the keys. Using an algorithm like the RSA which is public knowledge also means following Kerkchoffs second principle. The principle states that ”A cryptographic system should be secure even if everything about the system, except the key, is public knowledge” [29]. Adhering to this principle means adhering to open design of secure software systems. Hence we use RSA and not any custom made encryption algorithm [15].

Two large prime numbers are randomly picked. The public and private key are dependent on this selection. The public key is used for encryption. The private key is known to the intended recipient, and decryption is possible only by the intended party. Usually both the keys are generated at the receiver. Only the public key is communicated to the transmitter. The active warden will not be able to understand what is embedded inside the stego media because of the use of encryption.

Spread Spectrum Modulation:

The encrypted data is made further secure by using Direct Sequence Spread Spectrum (DSSS) Technique. The data is converted into a stream of bits and is spread over a broad bandwidth with the help of a spreading signal. This spreading over a large bandwidth makes the resulting wideband signal appear as a noise signal which helps create greater resistance to intentional and unintentional interference for the transmitted signal [30].

The database is a Pseudo Random Number Generator (PRNG) which generates long bit sequences known as Pseudo Noise (PN) sequence - a code with shorter duration (larger bandwidth) as compared to the data. The data is modulated with this PN code which is equivalent to chopping data into smaller pieces and spreading it over the large bandwidth. The smaller the chip duration of the PN code, the larger the bandwidth and therefore higher immunity to interference. The resulting signal is similar to white noise and has a bandwidth almost equal to the PN code. Attacks of information extraction become computationally complex as the message is now spread out.

Hash-based Message Authentication Code Generation:

A malicious warden might try to fake an identity in a communication channel. It is imperative for the communicating parties to verify the authenticity and integrity of the message. The proposed method accomplishes this by generating a Hash-based Message Authentication Code (HMAC) with the help of a cryptographic hash function called Secure Hash Algorithm (SHA). SHA is a mathematical operation which generates a hash value for a given input data. Following are the important reasons for using cryptographic hash functions for data authentication:

(1) Variable size input.
(2) Fixed size output
(3) Collision resistance - Each input has a unique output. There are no two x and y such that: H(x) = H(y). where H is the cryptographic hash function.
(4) Pseudorandom - The output sequence is entirely random.
(5) One way - It is not possible to find x given y that: H(x) = y. where H is the cryptographic hash function.

The cryptographic hash function used here is SHA-256. The output is a 64-character hexadecimal number which corresponds to 256 bits. HMAC is unique to the given input message. HMAC is essentially a unique digital signature of the message. Examples of HMAC using SHA-256 [31]:

(1) **Input message:** Hello
Output HMAC: 66a045b452102c59d840ec097d59d9467e1
3a3f34f6494e539ffd32c1bb35f18
(2) **Input message:** ’IhaveaDream.txt’ [32])
Output HMAC: 047488747b53209475291a30638400e73a0
038377f4e1aaab9edcb2d27270aaf

We can get to know of steganalysis attacks like modification and destruction with HMAC. A new HMAC will be generated for the message retrieved at the end. The generated HMAC must match with transmitted HMAC for authentication and data integrity. Any change in either the message sequence or the HMAC sequence will result in an unsuccessful verification.

(B) Insertion Strategy

Data Scrambler:

A data scrambler is a digital device that jumbles and encodes the message at the sender’s end to make it unintelligible at a receiver not equipped with a corresponding de-scrambling device. The HMAC and the wideband data stream are scrambled together through random permutation. This permutation further secures the system from detection attacks which aim to find meaningful portions of data inside a stego media. A passive warden will find it tough to conclude if meaningful data is present. It is essential that insertion strategy should offer a balance of 0s and 1s as well as be random enough so that it can mimic the LSBs of the cover image [10]. The modification attacks which involve destroying the message without damaging other aspects of the stego media become tough.

Video Steganography:

Figure 4 shows the data embedding algorithm used to hide the data in the stego media. The input media is a video stream. A video is a combination of two types of data - audio and image. Three types of steganography are possible for a video - only image, only audio, and combined audio-image. These options correspond to a larger room for error for the warden to conclusively state the presence of hidden information. In the event of a suspicion that steganography is taking place, a video proves to provide a higher level of secrecy.

Image Extraction—To minimize vulnerability, information in the proposed model is hidden only in the images. The audio stream is not used for steganography. Hence image frames are extracted from the video stream. This selection strategy helps prevent major changes in the statistical properties of the video thereby reducing the possibility of attracting the attention of an attacker. Additionally, a video being streamed at 30 frames per second and with 1 million pixels a frame sums up to a total of 30 million pixels per second (90 million pixels for a color image). This gives the algorithm huge space to hide the information. Videos with higher resolution streamed at higher frame rate prove to be even better.

Color Plane Selection—Another layer of security is proposed in the system by selecting only 1 out of 3 color planes (R G B or Y Cb Cr) in a given color model. This aids in the concealment of information as well as helps maintain the statistical properties compared to embedding information in

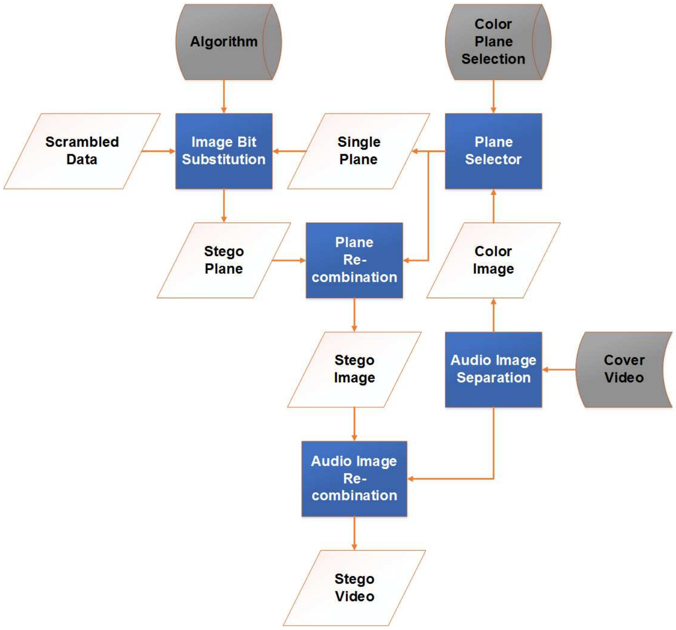


Figure 4. **Steganography - Data Embedding Algorithm**

all the three color planes. The strength of the algorithm lies in decreasing the probability of a change in the palette color values of each pixel and in minimizing the visual distortion that is introduced [33].

Algorithm—This algorithm forms the core of the proposed system. It specifies the type and manner of substitution of bits into the specified image color plane. The main idea is to add noise-like signal to the video pixels. This signal is below the threshold of perception [24]. Because we have used a Pseudo Noise (PN) signal for DSSS modulation, the embedded information is also noise-like and difficult to locate and extract. The algorithm can be made to follow particular functions which will aid in the process of seamless embedding of data.

Image Bit Substitution—In the LSB substitution technique, the information is usually hidden in a sequential fashion. Hence the risk of information being uncovered is high as it is susceptible to sequential scanning based techniques of the active warden. The Random Pixel Manipulation Technique attempts at overcoming this problem, where pixels are chosen in a random fashion instead of a sequential one [16]. Such techniques make it difficult for the active warden to detect information [17] [34]. It would be a smarter move to insert the message only into a subset of the available pixels. Figure 5 and Figure 6 show the random pixel allocation on a subset of pixels available in an image frame.

Each letter has N number of bits, where N depends on the length of the PN code. Each letter of a word is embedded as payload into a single color plane of each frame, with N pixels being modified in it.

Combination—After the image bit substitution, the untouched color planes are recombined with the stego plane. The audio is also combined with the stego image to produce the stego video which is then transmitted over the communication channel for the intended the recipient.

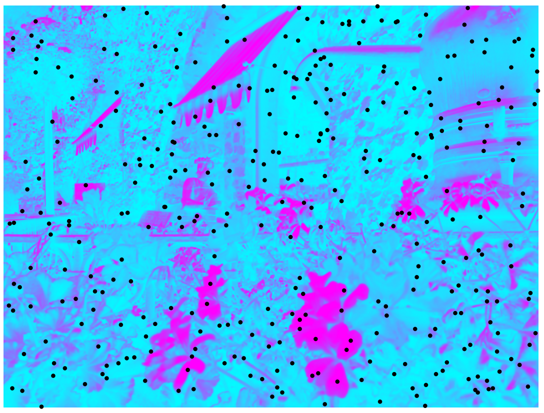


Figure 5. **Random Pixel Manipulation Technique in Blue plane with 350 pixels**

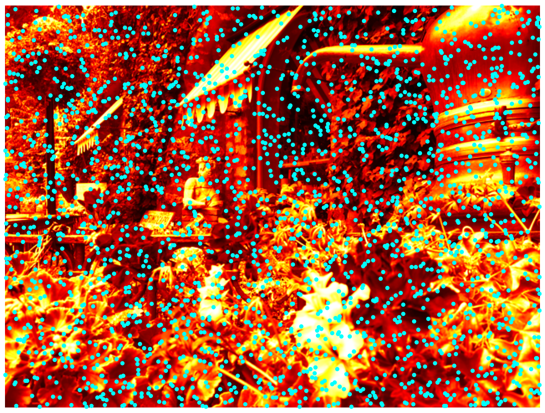


Figure 6. **Random Pixel Manipulation Technique in Red plane with 2100 pixels**

(C) Message Retrieval and Extraction:

Figure 7 lists the steps at the receiver end. It is essentially an inversion of the operations involved in the encoding process. The data extraction algorithm is separately illustrated in Figure 8. The original cover video is required for successful extraction of the secret message. The RSA Private Key, PN Code, Data De-scrambler, Color Plane Selector and Bit Extraction Algorithm are also needed for fruitful and error-free message extraction. The SHA-256 HMAC module is further used to ensure integrity and confidentiality of the secret message that is extracted.

(D) Performance Analysis:

Methods like PSNR and MSE calculate the absolute error. They assess perceptual image quality to quantify the visibility of error between the reference and modified image and are based on a variety of known properties of the human visual system. Structural Similarity Index was developed with an assumption that human visual system can detect structural changes in an image. It is based on an assessment of perceived change in the structural information of a scene, along with including luminance and contrast masking [35]. This index, therefore, gives an idea of structural similarity

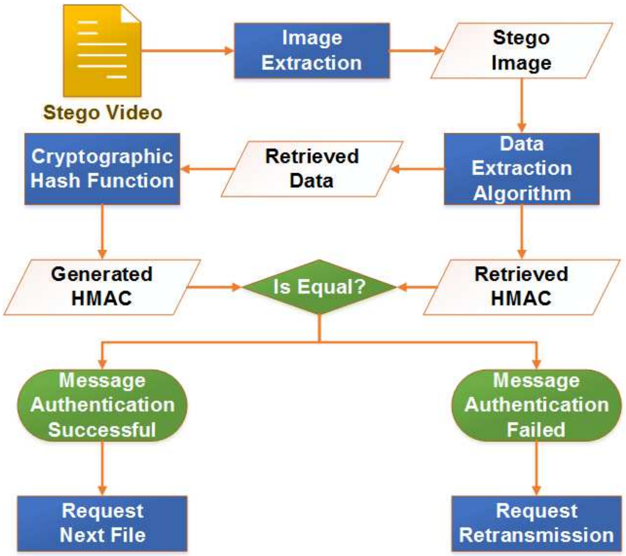


Figure 7. **Message Retrieval and Authentication**

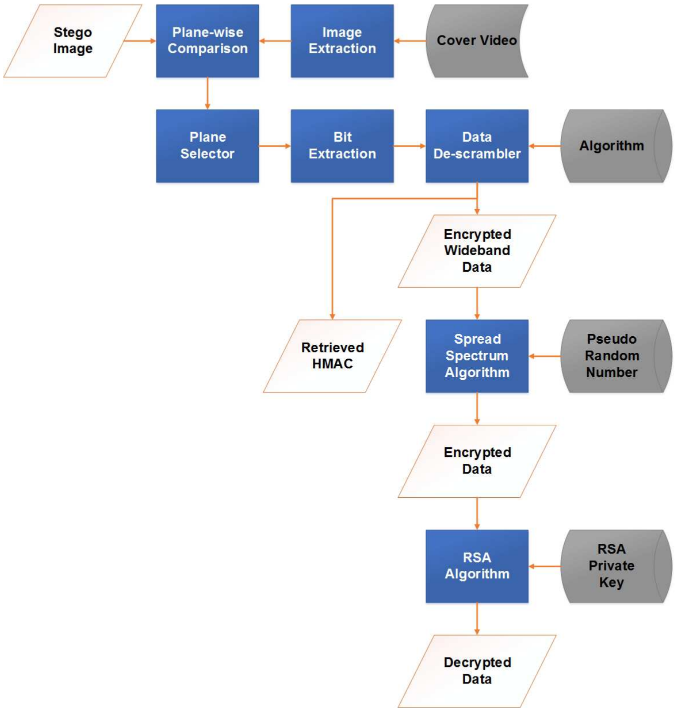


Figure 8. **Data Extraction Algorithm**

between cover and stego image.

All results presented were performed on a 0.3 MP image flowers.jpg. It is a Standard Definition (SD) color image with a resolution of 640 by 480 pixels. The original image is shown in Figure 9. A letter was embedded in each frame as per the proposed method. For illustration, letter I was embedded in the cover image. Figure 9 shows the stegoed image obtained after embedding 7000 characters into the cover image. The results indicate that there were no visual changes.

For a video of SD resolution running at 30 frames per second, Table 1 states the length of video required to embed each of the secret messages.

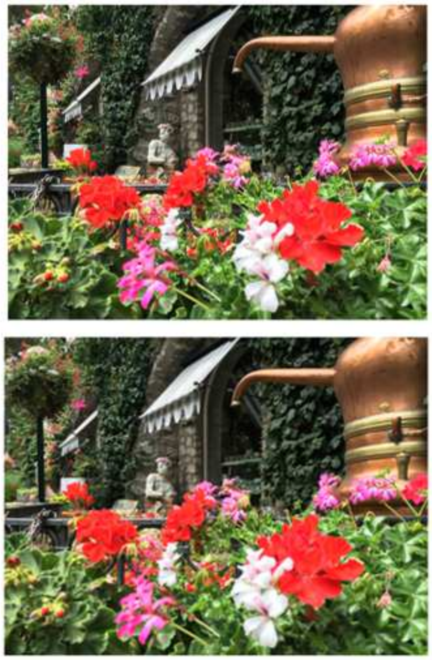


Figure 9. **Cover vs Stego with 7000 pixels modified**

Table 1. **Length of Stego Video**

No.	Secret Message	File Size	Video Length
1.	IhaveaDream.txt [32]	10 KB	320 secs
2.	Address.txt [36]	2 KB	58 secs

Various types of statistical analyses were performed on the stego image to give an idea of the efficiency of embedding algorithm. Table 2 depicts the change in parameters for letters ’I’ and ’P’ when no. of modified pixels are increased. Each letter is analyzed with different RSA keys. Figures 10 through Figure 13 summarize these results. The SSIM values are illustrated in Table 2. These values are very close to 1.0 even when 4000 pixels are modified. It means that the cover and stego image are structurally identical which is an essential requirement in steganography.

Table 2. **Image Parametes with change in length of PN**

L	MSE	PSNR	SSIM	% BER
5	5.2083e-05	95.7350	0.999999966	0.0114
10	1.2695e-04	91.8655	0.999999960	0.0227
50	5.7942e-04	85.2720	0.999999849	0.1139
100	0.00111328	82.4359	0.999999393	0.2278
200	0.00236328	79.1668	0.999998715	0.4557
500	0.00414388	76.7279	0.999998677	0.8138

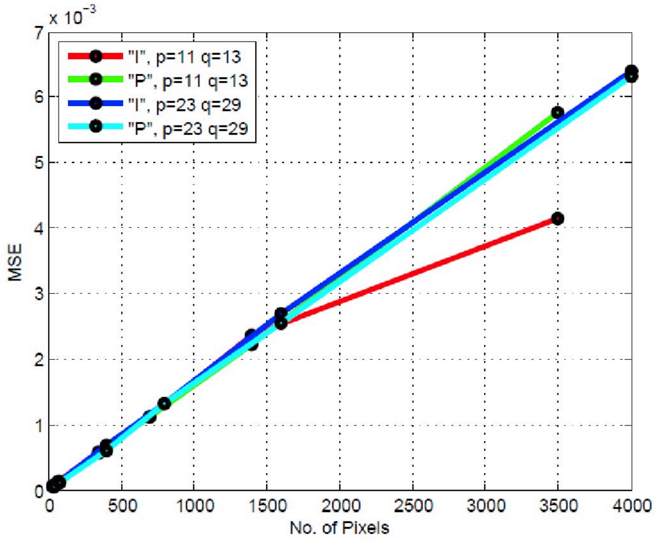


Figure 10. **Mean Square Error with change in pixels**

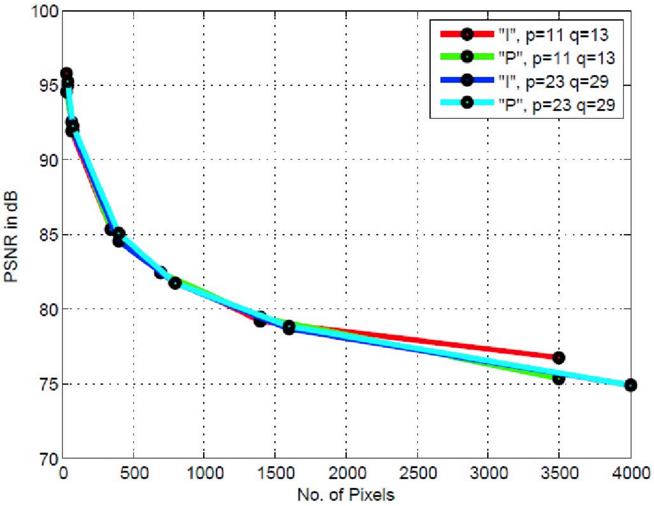


Figure 11. **Peak Signal to Noise Ratio with change in pixels**

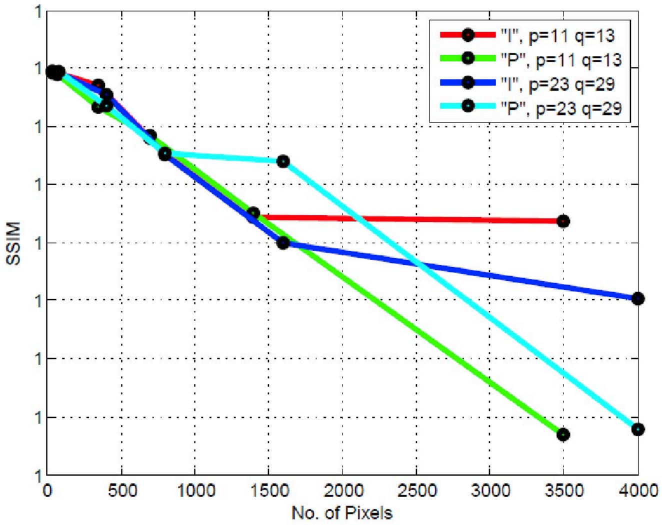


Figure 12. **Structural Similarity with change in pixels**

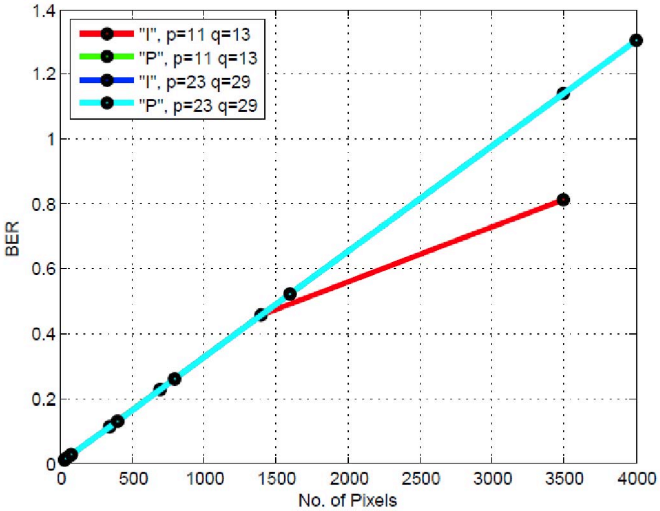


Figure 13. **Bit Error Rate with change in pixels**

5. Secured Inter-Satellite Communication

In satellite communication, signals are transmitted between sender and receiver with the help of satellites in space. It is a unique type of communication. The distance between sender and receiver is not a limiting factor. With the use of active satellites, a signal can be sent from one location on the globe to another. This makes satellite communication strategic from the viewpoint of national security. For example, a commander sitting at the armed forces headquarters can directly communicate in real-time to a remotely located mobile soldier on a mission. There are missions where signal connectivity is not present, or it is not desirable to route the communication via public networks. Satellite communication provides confidential end to end communication in such scenarios. Signals are relayed between a ground station (GWL) and satellite multiple times before it reaches the intended user (UML). This has a distinct disadvantage the number of uplinks and downlinks required increase drastically. Inter-Satellite link (ISL) can be used to overcome this bandwidth wastage. ISL is a direct connection between two satellites. Signals originating at a ground station are uplinked to a satellite in view. Then it is relayed via multiple ISLs to the satellite connected to the intended user. A network of satellites is used around the globe for the same, thus reducing the number of links required. Each satellite is provided with three links - the User Mobile Link (UML) for communication with a mobile station, the Gateway Link (GWL) for communication with an earth station and the Inter-satellite Link (ISL) for communication between two satellites, which are close to each other.Low Earth Orbit (LEO) satellite constellations can provide high bit rate interconnections, which enable them to provide low delay connections between two distant points on the earth surface [37].

There are thousands of satellites hovering around the earth at any moment. A signal can be intercepted during ISL, UML or GWL. Figure 14 shows an example of an adversary trying to intercept an ISL. Though tough and complex it is possible. It is important for countries to safeguard the information being sent via these links. Using steganography can help secure this communication link. An adversary who may want to intercept the channel finds nothing but innocuous media. It does not raise suspicion and not invite attacks as in the case when heavily encrypted data. The proposed hybrid system can be used to realize private and secure communication via ISL along with maintaining data integrity and confidentiality.

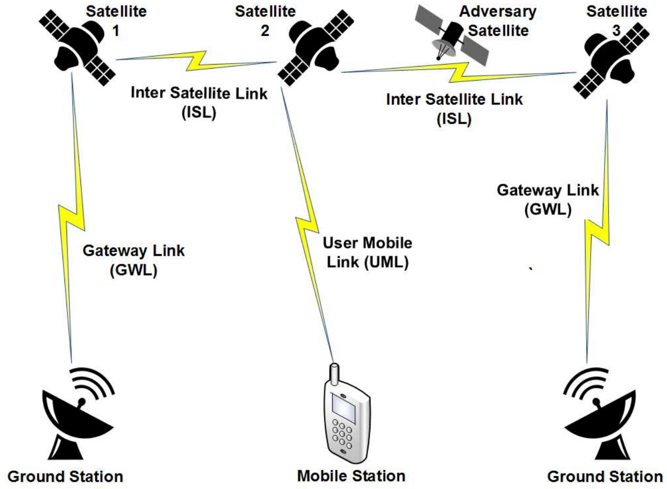


Figure 14. **Adversary Satellite in ISL**

6. Conclusion

The work presented in this paper is an effort to develop a robust Steganographic System. The proposed combination of techniques algorithm incorporates features from various existing techniques to form an efficient steganographic algorithm which can help in cover communication.

The science of Steganography requires that the cover image must be carefully selected. A familiar image should not be used for steganography. It is better for steganographers to create their cover media [10]. The aim of any steganographic algorithm to pass unnoticed [13]. The resulting stego image obtained contains minimal visually perceptible changes. This perceptibility is crucial because as discussed earlier, visual perceptibility (visual quality) is one of the critical parameters. The size of the payload is determined by the resolution and frame rate of the video. The RSA-encrypted message is modulated by a PN code. This information is scrambled randomly along with the HMAC of the secret message, adding randomness to the process. Then, this data is embedded into the LSBs of pixels of a particular color plane in each of the image frames of the cover video. Since information is present in all the three color planes of the video, no single plane carries meaningful information. This combination of techniques makes retrieving the hidden message from a video a tough task. The RSA keys, PN code, Plane Selector and Data Scrambling algorithms are needed, failing which extracting the information is useless. Further, the amount of payload inside each frame is kept strategically low not to raise suspicion and not invite detection attacks. As shown by the results, the statistical properties of low-density stego images are comparable to the cover image, thus giving no information on the presence of a secret message.

The secret message to be communicated can be compressed to maximize the net payload in a stego media. Compression algorithms work on the redundant data present inside a message by finding some patterns. An encryption algorithm will randomize the data, leaving no patterns. Hence, the payload should be compressed even before it is encrypted. Many types of lossless compression techniques can be used. Correlated Steganography can also be used to reduce the bits needed to encode a message [10]. The proposed method uses only image steganography. However, advancement in Voice over Internet Protocol (VoIP) and various Peer-to-Peer (P2P) audio services offer numerous opportunities for secret communication using audio steganography. Minor change in the binary sequence of audio samples with existing steganography tools can easily facilitate secret communication. Moreover, audio signals have an inherent redundancy and unpredictable nature which makes them ideal to be used as a cover media to hide secret messages in secret communications [33]. Similar techniques can be used to hide data inside the audio of a video stream. Interleaving is the reordering of data to be transmitted so that consecutive bytes of data are distributed over a larger sequence of data. Interleaving is done to reduce the number of burst errors. The use of interleaving significantly improves the ability of error protection codes to rectify burst errors. Usually, error protection coding processes can correct small numbers of errors and not the ones which occur in groups [38]. Forward secrecy feature can be applied to the public key encryption. A unique random public key without using a deterministic algorithm will be utilized for each session. Therefore, compromise of a given message does not mean a compromise of other messages. Moreover, there is no single way to compromise multiple messages together.

Steganography can be used for a wide variety of applications relating to national security. It can help aid the circulation of vital and classified information. The applications are numerous. For example, applying steganography in intelligent restricted Content Based Image Retrieval (CBIR) [39]. Steganography also has major advantages in inter-satellite communication where secret information needs to be shared but the risk of interception looms. However, there are some applications which can misuse this science [10]. Examples include the use by criminals to communicate with each other. The question whether child pornography exists inside seemingly innocent media files and whether robust stego files can bypass an anti-virus system to communicate hidden information are few among many disturbing questions which need to be addressed. However, it is clear without a doubt that steganography can be used for useful applications. Moreover, along with encryption, it becomes a formidable tool for private and secured communication [10].

Acknowledgments

The authors would like to thank the entire team at Quanical Innovation Lab for their constant support, valuable inputs and motivation given throughout the research project. We would also like to take this opportunity to thank all the anonymous reviewers for their time and valuable suggestions.

References

[1] Rivest, Ronald L. (1990), ”Cryptography”, In J. Van Leeuwen. Handbook of Theoretical Computer Science 1, Elsevier.

[2] Bellare, Mihir; Rogaway, Phillip (21 September 2005), ”Introduction”, Introduction to Modern Cryptography, p. 10.

[3] ”Overview per country”, Crypto Law Survey, February 2013.

[4] "UK Data Encryption Disclosure Law Takes Effect", PC World, 1 October 2007.

[5] Ranger, Steve (24 March 2015), "The undercover war on your internet secrets: How online surveillance cracked our trust in the web".

[6] K. S. Babu, K. B. Raja, K. K. Kiran, T. H. Manjula Devi, K. R. Venugopal and L. M. Patnaik, "Authentication of secret information in image Steganography," TENCON 2008 - 2008 IEEE Region 10 Conference, Hyderabad, 2008, pp. 1-6.

[7] L. M. Marvel, C. G. Boncelet and C. T. Retter, "Spread spectrum image steganography," in IEEE Transactions on Image Processing, vol. 8, no. 8, pp. 1075-1083, Aug 1999.

[8] S. M Thampi. Information Hiding Techniques: A Tutorial Review.

[9] The CRYSTAL project. Available from: http://bit.ly/2eiONGq

[10] Cheddad, J. Condell, K. Curran and P. Mc Kevitt, "Digital Image Steganography: Survey and Analyses of Current Methods". Signal Processing, Volume 90, Issue 3, March 2010, Pages 727-752.

[11] J. Cox, J. Kilian, F. T. Leighton and T. Shamoon, "Secure spread spectrum watermarking for multimedia," in IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673-1687, Dec 1997.

[12] P. Marwaha and P. Marwaha, "Visual cryptographic steganography in images," Computing Communication and Networking Technologies (ICCCNT), 2010 International Conference on, Karur, 2010, pp. 1-6.

[13] Mishra, A. Gupta and D. K. Vishwakarma, "Proposal of a New Steganographic Approach," Advances in Computing, Control, and Telecommunication Technologies, 2009. ACT '09. International Conference on, Trivandrum, Kerala, 2009, pp. 175-178.

[14] K. Zhang, H. y. Gao and W. s. Bao, "Steganalysis Method of Two Least-Significant Bits Steganography," Information Technology and Computer Science, 2009. ITCS 2009. International Conference on, Kiev, 2009, pp. 350-353.

[15] M. Juneja and P. S. Sandhu, "Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption," Advances in Recent Technologies in Communication and Computing, 2009. ARTCom '09. International Conference on, Kottayam, Kerala, 2009, pp. 302-305.

[16] S. Venkatraman, Ajith Abraham, M. Paprzycki, "Significance of steganography on data security", Information Technology: Coding and Computing, 2004.

[17] R. Chandramouli and N. Memon, "Analysis of LSB based image steganography techniques," Image Processing, 2001. Proceedings. 2001 International Conference on, Thessaloniki, 2001, pp. 1019-1022 vol.3.

[18] L. M. Marvel, C. T. Retter and C. G. Boncelet, "Hiding information in images," Image Processing, 1998. ICIP 98. Proceedings. 1998 International Conference on, Chicago, IL, 1998, pp. 396-398 vol.2.

[19] N. F. Johnson and S. Jajodia, "Steganalysis: The investigation of Hidden information," in International Conference on Information Technology, pp. 113116, Jun 1998.

[20] Y. Wang and P. Moulin, "Steganalysis of Block DCT Image Steganography," in International Conference on Image Processing, pp. 339342, Mar 2003.

[21] V. M. Potdar and E. Chang, "Grey level modification steganography for secret communication," Industrial Informatics, 2004. INDIN '04. 2004 2nd IEEE International Conference on, Berlin, 2004, pp. 223-228.

[22] H. Sung, G. R. Tadiparthi and S. Mukkamala, "Defeating the current steganalysis techniques (robust steganography)," Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International Conference on, 2004, pp. 440-444 Vol.1.

[23] P. Wayner, Disappearing Cryptography: Information Hiding: Steganography and Watermarking.

[24] F. Hartung B. Girod, "Copyright Protection in Video Delivery Networks by Watermarking of Pre-Compressed Video", Multimedia Applications, Services and Techniques ECMAST '97 Volume 1242 of the series Lecture Notes in Computer Science pp 423-436

[25] Available from https://en.wikipedia.org/wiki/Structural_similarity

[26] J. Fridrich, "Steganography in Digital Media: Principles, Algorithms, and Applications".

[27] I. Cox, M. Miller, J. Bloom, "Digital Watermarking and Steganography."

[28] R. Rivest, A. Shamir and L. Adleman, "Cryptographic communications system and method", U.S. Patent: 4 405 829 A, issued September 20, 1983.

[29] Kerckhoffs, "La cryptographie militaire", Journal des sciences militaires, vol. IX, pp. 583, January 1883, pp. 161191, February 1883.

[30] S. Haykin, "Communication systems (4th edition)", John Wiley & Sons, 2008 pp. 48899.

[31] Available from: http://hash.online-convert.com/sha256-generator

[32] Speech of Martin Luther King, Jr. , Available from: http://www.americanrhetoric.com/speeches/mlkihaveadream.htm

[33] N. Meghanathan and L. Nayak, "Steganalysis algorithms for detecting the hidden information in image, audio and video cover media", International Journal of Network Security and Its Application (IJNSA), Vol.2, No.1, January 2010.

[34] N.F. Johnson, Z. Duric, and S. Jajodia, "Information Hiding: Steganography and Watermarking - attacks and countermeasures," Kluwer Academic Publishers, 2000

[35] Z. Wang, A. C. Bovik, H. R. Sheikh and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," in IEEE Transactions on Image Processing, vol. 13, no. 4, pp. 600-612, April 2004.

[36] Speech by President Abraham Lincoln. Available from https://en.wikipedia.org/wiki/Gettysburg_Address

[37] E. Papapetrou, I. Gragopoulos and F.-N. Pavlidou, Performance evaluation of LEO satellite constellations with inter-satellite links under self-similar and Poisson traffic, International Journal of Satellite Communications 17,51-64 (1999)

[38] Available from: http://www.wirelessdictionary.com/Wireless-Dictionary-Interleaving-Definition.html

[39] X. Li, "Watermarking in secure image retrieval", Pattern Recognition Letters, vol. 24, no. 14, 2003 pp. 2431-2434.

Biography

Swadhin Thakkar *is currently a research fellow at Quanical Innovation Lab at Mumbai, India. His research areas span Cyber-Security, Networks, Embedded Systems and Machine Learning. He received his Bachelor of Technology from Veermata Jijabai Technological Institute (VJTI) at University of Mumbai. He majored in the field of Electronics and Telecommunications. He is an incoming graduate student at Carnegie Mellon University (CMU). Swadhin has worked on health technology projects with MIT Media Labs and Camera Culture Group. He has also worked at National Centre for Excellence in Technology of Internal Security (NCETIS) - an Initiative by Indian Institute of Technology, Bombay and Department of Electronics and Information Technology (Government of India) under Digital India Program. His work included research and development of a Remotely Operated All-Terrain Vehicle for security and surveillance. He has also worked on projects in the field of embedded systems, circuit design, and computer vision. He is a recipient of the 'Sir Ratan Tata Trust Scholarship' and 'R. D. Sethna Scholarship Fund' for excellent overall performance.*

Kaustubh Shivdikar *is currently a Research Fellow at the Quanical Innovation Lab and Solutions Architect at Quanical Technologies Pvt. Ltd. Kaustubh has been in the field of Network Security for a long time. His latest work engulfs risk assessment of cryptography algorithms, especially DES, RSA, and HASH. He is the youngest student from his college to represent it at three international conferences including TED, Indian Science Congress and AeroConf 2016. Exploring the depths of artificial intelligence, he is currently working on Network Intrusion Detection using Artificial Immune System. He was an integral part of the MIT Media Lab India Initiative where his work revolved around Augmented Reality based projects like the Magic Pillow and ARtifact. Bagging a scholarship at the national level, he has received the National Talent Search Examination (NTSE) Award. He has previously worked in close associations with MIT Media Lab, Harvard Medical School and the University of Massachusetts Lowell as a research intern. An entrepreneur with a startup of his own, Kaustubh has received the Innovation Award at Maker Fest India.*

Chirag Warty *is currently the CEO of Quanical. He is also the Chief Scientist at Quanical Innovation Lab. He manages an extensive network of research teams in the US and India. He received his Bachelor of Science in Electrical Engineering from University of Mississippi, USA, Masters of Engineering from University of Illinois Chicago, USA. His other alma maters include Stanford, Cornell, Univ. of Illinois Urbana-Champagne (UIUC), UCLA, UC Berkeley, UC San Diego, USC. He also has several academic accolades in communications and signal processing from several IEEE societies. He is a visiting faculty for University of Mumbai, VJTI, and SNDT University for management, IT, and engineering programs. He currently manages several projects and is responsible for technology related global strategic decisions. His research interest includes Software Defined Networking (SDN), 4G/5G wireless technologies and Cyber-Physical Systems, Big data in Mobile Cloud Computing, Physical Layer Security. He has organized several panels and hosted forums on various technical subjects. He is a well-published author with several international publications and is a well-renowned speaker for future technologies. He holds several key and executive positions on IEEE societies. He is currently the guest editor for Elsevier's Special Issue on Big Data Inspired Data Sensing, Processing and Networking Technologies. He serves on the editorial boards of IEEE and non-IEEE ventures. He has also served as chair, co-chair (general or TPC) and international advisor in various IEEE conferences around the globe.*