

# A Study on Authentication Framework by using 2-D & 3-D Image/Video Based Encryption

Mr. Shailesh Kumar, Ph.D. Research Scholar, JITU

Dr. Yogesh Kumar Sharma, Professor, Department of CSE, JITU

Dr. Keshava Prasanna, Professor, Department of CSE, CIT Tumkur

**Abstract:** Steganography is the art and science of hiding sensitive data inside an image. There are so many cryptosystems that use Steganography as a major tool. Also in recent years there is a rising trend towards chaotic sequence based cryptosystems. A novel geometric framework is proposed for analyzing 3D faces, with the specific goals of comparing, matching, and averaging their shapes. Here we represent facial surfaces by radial curves emanating from the nose tips and use elastic shape analysis of these curves to develop a Riemannian framework for analyzing shapes of full facial surfaces. This representation, along with the elastic Riemannian metric, seems natural for measuring facial deformations and is robust to challenges such as large facial expressions (especially those with open mouths), large pose variations, missing parts, and partial occlusions due to glasses, hair, etc. From a theoretical perspective, this framework allows for formal statistical inferences, such as the estimation of missing facial parts using PCA on tangent spaces and computing average shapes. In this paper, attempts are made to combine the two with a new algorithm for data hiding. Here key images required for Steganography are generated using chaotic sequence. Also an attempt is made to overcome the limitations of Steganography on the file size ratio and the security offered by Steganography.

## INTRODUCTION

One of the significant changes required being developed is industrialization, which is the way to rebuild the economy. It is the headway of a group alongside including new and better strategies for creation and growing the span of the firm. Industrialization has ended up being a powerful instrument of development and welfare. It has been characterized as a procedure in which changes of arrangement of key generation capacities are occurring. It includes three fundamental changes that go with industrialization, motorization of an endeavor, working of another market and misuse of another region. When we dive deep into the procedure of industrialization the examination of different operational parts of the firm gets to be distinctly basic on the grounds that a firm is the constituent unit of each industry and henceforth, assumes a key part in the industrialization, where as an industry comprises of firms delivering indistinguishable or close substitutes for a few and moderately far off substitutes for every single other yield. Any such subgroup might be called industry. In the adventure to monetary development of an economy, producing segment assumes an urgent part. Consequently, the significance and need to assess this part is legitimized.

The digital images in the field of steganography algorithm have a major difference between spatial and frequency domain schemes is the convenience of implementation, the two approaches can provide different functions to cope with various applications. Generally, frequency or transform

domains of steganography schemes tend to achieve a better balance between robustness, security and fidelity than spatial domain.

## Brief History of Cryptography

With the latest development in information technology in data innovation and the high utilization of information on Internet, the requirement for data security has expanded in the current past. There are two principle branches of data security – Cryptology and Data Hiding. Both these branches have interested individuals since hundreds of years and various reviews have attempted to disentangle their secrets. Cryptology is a blend of two ranges: Cryptography and Cryptanalysis. Cryptography is the investigation of plans utilized for encryption and Cryptanalysis is the investigation of strategies utilized for interpreting a message with no learning of enciphering. Cryptology has customarily been utilized for security, protection or classification of correspondence over an uncertain channel. Since the scrambled information is incoherent, it is not avoided the busybodies.

## Image Cryptography

Cryptography is an effective way for protecting sensitive information as it is stored on the media and transmitted through un-trusted network communication paths. The applications such as ATM cards, computer passwords, online bank transaction, electronic commerce and group-oriented applications like video conferencing mainly depend on cryptography. The core of cryptography lies with the keys involved in encryption and decryption as well as maintaining the secrecy of the keys. Another important factor is the key strength, i.e. the difficulty in breaking the key and retrieving the original information.

## History of Steganography

Information hiding is a science which dates back to 1499, and it has long history. It has been used in various forms for 2500 years. It has found use in military, diplomatic, personal, spies, ruler, governments etc down through the age. Here following is the historically development of information hiding techniques such as steganography and watermarking. In the current corporate situation information or data security is the most significant source since loss of data will prompt to money related and advertise misfortune which thus will bring about the finish of business.

#### *Present perspectives of Information Hiding Techniques*

Adelson represented a technique for information concealing that adventures the human visual framework's differing affectability to differentiate versus spatial recurrence. He substituted high spatial recurrence picture information for shrouded information in a pyramid-encoded still picture. While he could encode a lot of information proficiently, there was no arrangement to make the information resistant to discovery or expulsion by commonplace controls, for example, sifting and rescaling. Drinking spree adjusted Adelson's method by utilizing disorder as a way to scramble the implanted information, preventing recognition, however giving no change to resistance to host flag control.

According to Xia et al. 1998 proposed a watermarking plan in the wavelet space in their review watermark was inserted as an irregular succession in the extensive coefficients in center recurrence groups. The interpreting procedure required the first picture and depended on various leveled connection of coefficients at various sub-groups. The proposed plan was appeared to be hearty against contortion brought about by separating or pressure. Wonder et al. 1998 concentrated spread range and blunder control methods to cover up and recoup messages into pictures. In their review the measure of added substance irregular commotion was controlled with Wiener channel in view of the provincial insights of the picture. Johnson and Biggar (1998) looked into changed watermarking approaches for advanced video and proposed another change space system that can be utilized information randomization preceding the addition of a stamp which included the adjustment of chose change coefficients. In their review the execution comes about demonstrated effective recuperation of the stamp and heartiness of the plan against advanced to simple and simple to computerized transformation.

#### *Differences between Steganography and Cryptography[1][7]*

This nature hiding information in cipher protects the message, but the interception of the message can just be as damaging because it gives clue to an opponent or enemy that someone is communicating with someone else. Steganography brings out the opposite approach and tries to hide all evidence during communication. The differences between steganography and cryptography are:

1. Steganography hides a message within another message normally called as a cover and looks like a normal graphic, video, or sound file. In cryptography, encrypted message looks like meaningless jumble of characters.
2. In steganography, a collection of graphic images, video files, or sound files in a storage medium may not leave a suspicion. In cryptography, collection of random characters on a disk will always leave a suspicion.

#### *Spatial Domain Data Hiding Techniques*

Nowadays, the transmission of digitized medical information has become very convenient due to the generality of Internet. Regardless of the prevention of medical fault, the real-time detection of abnormal event, the support of clinical decision, even the model developing of medical service based on patient, Internet has created the biggest benefit to achieve the goals of promoting patient safety and medicine quality.

#### *Overall Contribution of data hiding with Other Works*

Another critical criterion is the estimation of embedding capacity which is a measure of how much of information could be packed or embedded inside the image without causing any visual degradation or affecting the fidelity. The embedding capacity issues discussed by Servetto *et al.* (1998) have provided an insight into the various aspects of increasing the embedding capacity given a cover image. Brian Chen *et al.* (2000) have established a tradeoff between the embedding capacity and quality of watermarked image through his quantization index modulation methods (QIM). Weng .S *et al.* (2007) propose a distortion less image data hiding algorithm based on integer wavelet transform that can invert the stego-image into the original image without any distortion after the hidden data are extracted.

#### IMPLEMENTATION

This section describes the process for the implementation of the proposed data security system, activities performed to test the system, Camouflaging the Object, Image generation, Image exchange module, Encryption Module, Decryption Module, and the proposed framework for analyzing 3D faces under expressions, occlusions and pose variations.

#### *Camouflaging the Object*

Camouflaging is hiding the presence of a person, animal, or objects using camouflage. Where camouflage is the process of hiding something by painting or covering to make them blend with the surrounding. Camouflaging is the key feature of any country's defense system and their victory is largely depends how easily and effectively their soldiers can hide themselves at the war field. Camouflaging the object is the first stage in the algorithm for the implementation of the proposed idea for communication.

#### *Histogram Development*

The image files can be in many formats such as, JPEG (Joint Photographic Experts Group), EXIF (Exchangeable image file format), TIFF (Tagged Image File Format), BMP file format (Windows bitmap), PNG (Portable Network Graphics), and GIF (Graphics Interchange Format). However each one of them have one thing in common that these can be read in its components (CMYK or RGB). The images are read and its components are plotted against the pixel position along the X-axis. This set of graphs forms the histograms of the image. The histogram is a diagram that consists of rectangular sections having an area with respect to the frequency of a given variable and width with respect to the class intervals. In the camouflaging process, histogram is developed for all colors and light intensity.

#### *Obtain the Position of Source of Light*

After creating a histogram for the object of interest the next step is to obtain the position of the source of light. Every object cast their shadow when light falls on them. Therefore, we can find the position of the source of the light by using the shadow cast by the object.

### *Averaging Histogram*

In step 1 of the process we have created a histogram of the object for color and light intensity and in the above step we found out the position of the source of light, now we need to calculate the mean point of the light intensity. To do so, we calculate the average for all the points on the histogram. Then the new values are stored back into the image. This results in a flat image where the light intensity no longer produces the depth (3-d perception) to the image.

### *Averaging Color Histogram*

After we have calculated the mean of the light intensity, the next step is to find out the mean for the color histogram. The process followed is similar to what we followed for light intensity histogram.

### *Above and Below average*

In the above steps, we have calculated the averages for both the histograms, now we have to find the above and below average points for these histograms. This can be achieved by checking the frequencies at different points in the histograms. The points that are nearest to the mean or in other words that have frequencies just higher and lower than the mean point are taken.

### *Counter Shade*

Taking the values from the above steps, now we have to counter-shade the object. This will blend the object with the background or in simple words make it invisible.

### *Retrieval of the Object*

Once we have done the camouflaging of the object of interest, the sender sends the file to the intended receiver. As the key object is hidden, therefore our message is secured. Now the question arises the received image is not readable for the receiver as well. Hence, required some processing to interpret the original message. This is achieved at this stage.

### *Image Reconstruction*

The received image is firstly reconstructed using the maximum intensity point, intensity, and slope. These values can be identified from the histograms. The steps for reconstructing are:

1. Add the intensity into the image at the given point.
2. Obtain the other points on the image using the slopes in all directions.

### *Color Correction*

The reconstructed image is then processed for its color correction using regression analysis for high and low points. In regression analysis, we estimate the relationships among variables. It is a technique, in which, we fix the values of the dependent variable and then find out the estimate a conditional expectation of a dependent variable. In simple words, using this technique we find out the average value of the dependent variables by keeping the independent variables as fixed.

The steps followed are:

1. Obtain a full set of low points and high points for each pixel using a deviation constant.
2. Generate two images using these two sets.

### *Judging the right image*

The two images created above then undergo a visual identification process. They are examined for the object of interest. We compare both the images take the one which is closer to the original.

### *Image Generation*

The implementation of the suggested system is divided into four modules, out of which the first module is image generation.

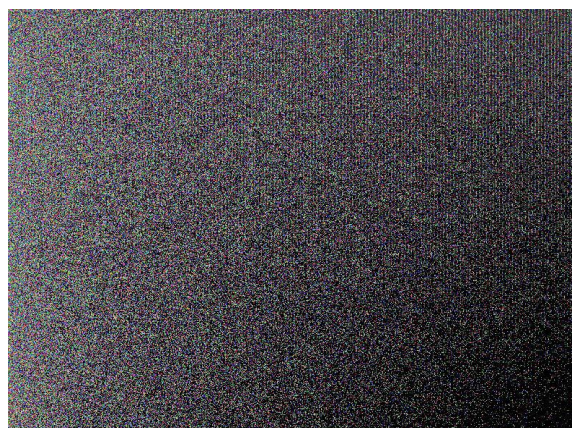
Chaos is mainly a state of disorder. In dynamical system, chaos is having a property such as sensitive to initial conditions. Due to the rapid development in the digital image processing and network communication, electronic publishing and wide spread dissemination of digital multimedia data have been communicated over the Internet and wireless networks. A chaotic sequence is generated deterministically from the dynamical system in which initial data grow apart.

The chaotic signals have many properties that are similar to some of the cryptographic properties such as:

- The Chaotic signals have the periodicity property which is similar to the confusion property in cryptography.
- The sensitivity of the chaotic signals is very high to their initial conditions or system parameters which are similar to the diffusion property of cryptography.
- The chaotic sequences also have noise like behavior and this is almost similar to the key sequences used in cryptography.

The trajectory of the chaotic system is totally unpredictable and highly random because of its highly sensitive response of chaotic systems to initial conditions.

The Chaotic system is sensitive to initial conditions, generates apparently random behavior but at the same time is completely deterministic. One can always obtain the same set of values for the same mapping function and an initial value. These properties of chaos have potential and promising application in designing a new Authentication Framework.





A sample of generated image using chaotic sequence for pixels. The above image looks like a noise, however, it is an image created a chaotic sequence of numbers. In the above image, the image header is written into a key file having 53 bytes (for .bmp format). Then, the pixels are loaded with 24-bit random numbers that make up Red, Green and Blue colors in each pixel.

#### Image Exchange module

Communication is one of the key factors persuading involvement of information between people by decreasing the distance between the people communicating. This communication has to be secure in order to keep concealed.

In this module, the images generated are exchanged between the pair of users as the title suggests. Each time a pair of users decides to use this system, before communication they use the image generation module and exchange the images. The image set can be exchanged physically/offline or online via a secure channel. In this paper, we have generated 10 images per set and 6 possible hop lengths per image. So, each set can be used for 60 independent communications between the pair.

#### Encryption Module

In cryptography, encryption is a method of coding a message or data in such some way that solely licensed parties will access it. Encryption doesn't of itself stop interference, however, denies the intelligible content to a would-be attacker. In AN encryption theme, the supposed data or message stated as plaintext is encrypted via a coding formula, generating cipher text which will solely be browsed if decrypted. For technical reasons, encryption theme mostly uses a pseudo-random coding key generated by a formula. It's in theory potential to rewrite the message while not possessing the key, but, for a well-designed coding theme, significant process resources and skills needed. A certified recipient will simply rewrite the message with the key provided by the creator to recipients, however, to not unauthorized users.

There are two types of encryption in general:

1. Symmetric key or private key encryption
2. Asymmetric or public key encryption.

In Encryption algorithm, a key is used to scramble the information using complex mathematical process. In Symmetric Key encryption type, only one key is used which is same for both the encryption and decryption process. However, in the Asymmetric or public key encryption process, two different keys are used for the encryption and decryption process. In this, the key used for encryption is a public key and the key used for decryption is a private key.

The most commonly used symmetric key encryption techniques are:

Data Encryption Standard (DES): It is a Symmetric-Key block cipher algorithm. It is a Feistel Cipher and uses 16 round Feistel structure having a block size of 64 bit.

The plaintext is processed in the following three phases:

1. The input plaintext is permuted using Initial Permutation IP. These permuted 64 bits are then divided into two 32-bit halves called L and R.
2. Then, 16 identical rounds are followed which consist of both permutation and substitution functions. Each round uses different sub key that is generated from the key. A function  $f$  processes the R part and the sub key. The output of this process and the L part are exclusive-OR to create the new R part. The new L part is simply a copy of the incoming R part.
3. After round 16, the L and R parts are exchanged and then the inverse of the initial permutation is applied to get 64-bit cipher text.

#### Decryption Module [4]

After the image is encrypted the sender sends the image to the authorized/appropriate user. In this module, the image received (containing the hidden message) is first used to get the key image ID and the hop count. Then it is exported with the key image file in the image set having the same ID and the bits at the hop count are written into a file. This file forms the decrypted message.

### RESULTS AND DISCUSSION

The algorithm is applied to a set of images having a small object of interest in a large landscape as background and the results are shown in Table 4.1. It is evident from the table 4.1 that our algorithm works as expected. However given the nature of the image and the background, it has its limitations. It can perform well on images with large majorly monochromatic backgrounds where as its performance will be diminished when applied on images that have vibrantly colorful backgrounds. The results are analyzed in the next section for visibility at each phase of the algorithm and the analysis reveals that with fine tuning and tweaking our algorithm can deliver the best invisibility in image to the objects of interest, in this case soldiers who are forced to use open data lines for image based communication.

The receiver end process details are given in table. It can be seen that in most cases, as the source of light is above (the sun), the lower points provide the object of interest. The reconstruction of the image is successful in all the cases from table.

The analysis of the performance of our algorithm is carried out by comparing the visibility of the Object of Interest before and after applying the proposed algorithm.

The computation of visibility of an object  $x$  is done using

$$V(x) = \frac{I(x) - I_B(x)}{I_B(x)} \quad (1)$$

Where  $V$  is the visibility (contrast)[8] and  $I(x)$  is the light intensity at  $x$  and  $I_B(x)$  is the average intensity of the background. The result of the comparison is as shown in table

1. From the table 1 it is evident that the algorithm achieves camouflaging but under the assumptions as follows

1. Single light source
2. Largely monochromatic background
3. Object of Interest is already using physical camouflage

Case	I	I <sub>B</sub>	Prior to TCS	I	I <sub>B</sub>	Post TCS
4.1.1	0.63	0.47	0.3404	0.5	0.47	0.0638
4.1.2	0.72	0.48	0.5	0.63	0.46	0.3695
4.1.3	0.54	0.46	0.1739	0.52	0.46	0.1304
4.1.4	0.86	0.53	0.6226	0.68	0.53	0.2830

Table 1: Visibility test performed on images before and after counter shading (TCS)

But it can be seen that this will not be the case in real life as practically one cannot expect all the assumptions to be adhered to. If an image falls into the hands of eavesdroppers/men in the middle without the keys i.e. the maximum intensity point and slopes, it will be very difficult to obtain the position of the object of interest in the image. The following Table 2 shows the time required to obtain the object of interest (not the reconstruction of the entire image) for the same cases in Table 1









TCS Image	Reconstructed Image Without keys	Object of Interest (Y/N)	Time Taken (s)
		Not obtained (N)	1.281
		Visibility improved (Y)	1.322
		Visibility reduced (Y)	1.098
		Visibility improved (Y)	1.024

Table 2: Unhide attempts on the TCS images using brute force method

The analysis also indicates that the system is breakable if the attacker has copies of all communications and by happenstance obtains the same key image used repeatedly. The occurrence of this demands that the attacker monitors each and every communication between the pair of users. Hence the possibility of the system being cracked is very low. The regression analysis shows that the relevance between Plain text and Cipher text for a 1 kB text file is less than 0.18 using the Pearson Product moment correlation. This shows that a simple backtracking method will not succeed in breaking our method.

## CONCLUSION

The work aimed at developing a system for effectively hiding objects in an image so that they can blend into the background seamlessly. The goal has been achieved successfully. The limitations of the algorithm have been explored and they can be corrected with further tweaking of the modules of the algorithm. The system can be improved upon by statistically analysing its performance with larger sets of data and applying non-linear regression to obtain the color averages. Also the output can be taken as an intermediate image and multiple iterations can be carried out to enhance the performance. Our algorithm, we hope can be used by the departments of defence of any country to carry out communications even in open channels without risking detection by enemies.

From our work it can be concluded that, Steganography, even though shunned as old, can be altered to prove very useful. The tweaks and added features that we have shown in this paper make sure that the communication is safe and secure if only the pair of users can maintain the key files are safe and offline all the time. Thus our proposed system works better on any type of file with any operating system. It also fares well against most of the known cryptanalysis methods.

Hence it proves to be an efficient and universal steganography system for individual as well as organizational users for pair wise communication.

- This also opens up a line of research for developing methods based on our work to have the following features. Larger key sets with verifiable randomness
- Sequential steganography of larger files using multiple key images
- Design and development of a server to function as arbitrator of generalised system, to overcome the limitation of pair wise communication.

## REFERENCES

- [1] S. Lian, Multimedia Content Encryption: Techniques and Application, CRC, 2008.
- [2] C.-P. Wu, C.-C. J. Kuo, "Design of integrated multimedia compression and encryption systems", IEEE Trans. Multimedia, vol. 7, no. 5, pp. 828-839, 2005.
- [3] Adam J. Slagell. Known-Plaintext Attack Against a Permutation Based VideoEncryption Algorithm. Available from <http://eprint.iacr.org/2004/011.pdf>.
- [4] L. Tang, For encrypting and decrypting MPEG video data efficiently," in Proceedings of The Fourth ACM Intl. Multimedia Conference (ACM Multimedia), (Boston, MA), pp. 219-230, November 1996.
- [5] T.B. Maples and G.A. Spanos, "Performance study of selective encryption scheme for the security of networked real-time video," in Proceedings of the 4th International Conference on Computer and Communications, Las Vegas, NV, 1995.
- [6] C. Bergeron and C. Lamy-Bergot, "Compliant Selective Encryption for H.264/AVC Video Streams," in Proceedings of the 7th IEEE Workshop on Multimedia Signal Processing, 2005, pp. 1-4.
- [7] Shiguo Lian, Zhongxuan Liu, Zhen Ren and Haila Wang, "Secure Advanced Video Coding Based on Selective Encryption Algorithms," IEEE Transaction on C