Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 3, Issue 5, May-2016

An Efficient Video Encryption Technique using Chirikov Standard Map

A. Ponkia[1], K. Kareliya[2]

Assistant professor, Dept. of ECE, S.S. Engineering College, Bhavnagar, Gujarat, India[1]

PG Student [Communication Engineering], Dept. of ECE, S.S. Engineering College, Bhavnagar, Gujarat, India[2]

ABSTRACT

As the trading of information over the open systems and Internet is quickly developing, security of the information turns into a noteworthy concern. In open system, it is essential to keep touchy data secure from getting to be defenceless against unapproved access. One conceivable answer for this issue is to encrypt the information. The information can be content, picture, sound, video etc. In today's world a large portion of the mixed media applications include pictures and video. Encryption is utilized to guarantee high security for Images. Chaos has been generally utilized for picture encryption for its diverse elements. There is numerous chaos based encryption strategies. The greater part of the proposed discrete riotous cryptographic methodologies depends on stream or block plans. In the event that these two plans are joined the security level is made strides. Chaotic maps give favourable circumstances of vast key space and abnormal state security. one of the well-known method of Chaotic map is Chirikov standard map has been used here.

The given methodology is exceptionally basic, quick, precise and it have been connected together as a twofold calculation keeping in mind the end goal to serve best results in very unsecure and complex environment.

KEYWORDS: Video Encryption, Encryption using Chirikov, security, video processing, System Security.

I. INTRODUCTION

The significantly spreading of the correspondence systems over the world expanded reliance on digitized data throughout our life. Subsequently computerized data is more important now days this advanced data contain mixed media information comprise of picture, sound, video, content, and so on. In upcoming days, the utilization of sight and sound information on web is going to increment because of the advancement of computerized and media innovation. The advanced pictures get to be a standout amongst the most imperative data transporters which are useful for validation, Biological science, military, internet keeping money exchanges, web shopping, online individual photo collection, and so on. Video Encryption method is totally differing to that of text encryption method. More established algorithms, for example, DES, IDEA, AES, 3DE S and so on are not reasonable for images, videos and representation because of information limit, solid neighbouring pixel relationship and high redundancy which minimized the encryption execution.

Video Encryption is the procedure of changing data (alluded to as set of back to back plain-image) utilizing a calculation (called cipher) to make it incoherent to anybody aside from those having unusual information, ordinarily alluded to as a key. The consequence of the procedure is encrypted image (alluded to as cipher-image). Decoding is the procedure of changing over cipher-image once again into its unique different structure, so it can be identified.

Video Encryption can be utilized to ensure Pictures (belong to extracted frames from video) very still, for sample, frames on PCs and capacity gadgets in a circumstance which individual records being uncovered through misfortune or break-in of portable PCs or strengthening drives. Image encrypting very immobile protections them from being revealed and shared. Encryption is likewise used to ensure information in travel, for instance information being exchanged by means of networks (e.g., the Internet, e-trade), mobile phones, wireless frameworks, Bluetooth gadgets etc.

Chaos is suitable for image encryption, as it is closely related to some dynamics of its own characteristics. The behaviour of the chaos system, under certain conditions, presents phenomena which are characterized by sensitivities to initial conditions and system parameters. Through the sensitivities, the system responses act to be random. The main advantages of the chaotic encryption approach include: high flexibility in the encryption system design, good privacy due to both nonstandard approach and vast number of variants of chaotic systems, large, complex and numerous possible encryption keys and simpler design. The digital image processing methodology is classified into two

categories- pixel value substitution and pixel location scrambling. The first one concentrates on changing the pixel value so that others cannot read the original pixel information in the digital image.

In this paper, we propose another quick calculation to be utilized as an encryption calculation which depends on predefined examine designs for rearranging the pixels of image and straightforward fundamental encryption function.

II. PROPOSED METHOD

In Chaos based encryption, the process is mainly performed on pixels. We know that pixels are the minute part of the frame. Thus to perform any operation on the frame, one has to perform all the task on whole pixels of the image. Thus in order to encrypt a video, video should be converted into frames. All frames or images should be kept to do process as to encrypt the video. And iteratively to encrypt an image one has to perform encryption on all of the pixels of each and every frame.

Consider a Compressed video only to process on that. Now, as we do image encryption for particular images, the same way we will do the video encryption, by performing the same for a particular frame. The video required for this process is assumed to be of fixed length. Now we know that in Chaos based encryption technique there is various types of maps in form of real as well as discrete domain. Chaos means randomness. In this method generally location of pixels is being shuffled. Thus for a particular frame each of the row and column (full of pixels) are being randomized. This randomization has some particular unique pattern. But it is known up to other end or decryption side only.

Now consider a frame belongs to a compressed video and we are going to process on it pixel by pixel. This image is mainly of the size m*n. Initially the RGB matrix of the same frame has to be separated. After the separation, each of the matrix value R, G, B is being saved in three different frame to perform operations. Each frame is of the same size of that of in image. After separation each frame of R, G, B matrix is stored in L, A, B colour space respectively. The change of A, B value in the LAB colour space doesn't create that much variation as compared that much into the RGB matrix. Then the frames containing L is being encrypted. In this encryption, each of the pixel corresponding to L frame is being encrypted fully. Each row and each column is being scanned to encrypt each and every pixel of the L frame. The equation for that is;

```
a = K*sin((2*pi*i)/m);
b = i - j + uint16(a);
```

equation shown over here is with some of the portion of coding done for iteration of encryption technique for R image.

After encryption of R, the next of G and B is being Encrypted. After the completion of RGB encryption, the encryption of L is being done.

III. EXPERIMENTAL RESULT

In this scheme, particular video which is taken is of 21 frames. So, here outcomes for the first frame K=1 is taken with different result. The results are shown over here is in two spaces like RGB and LAB. Here comparison of RGB and LAB colour space is shown.

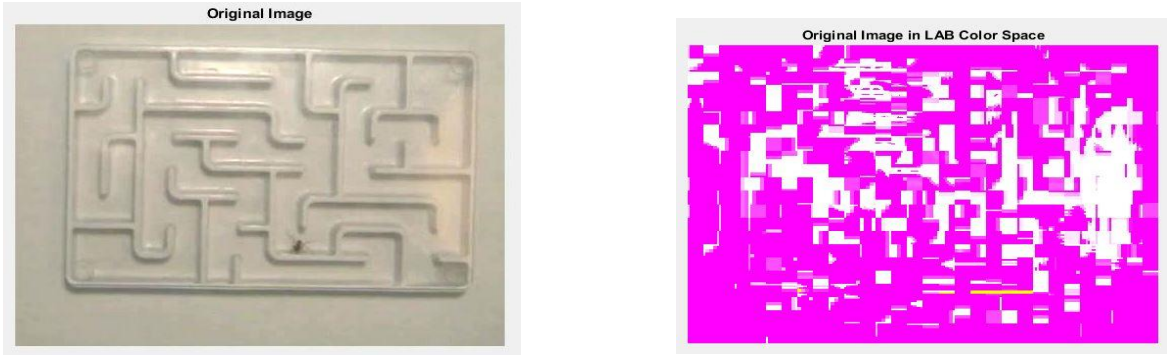


Fig. 1 Original image in RGB vs LAB

Fig. 2 Encrypted image in RGB vs LAB

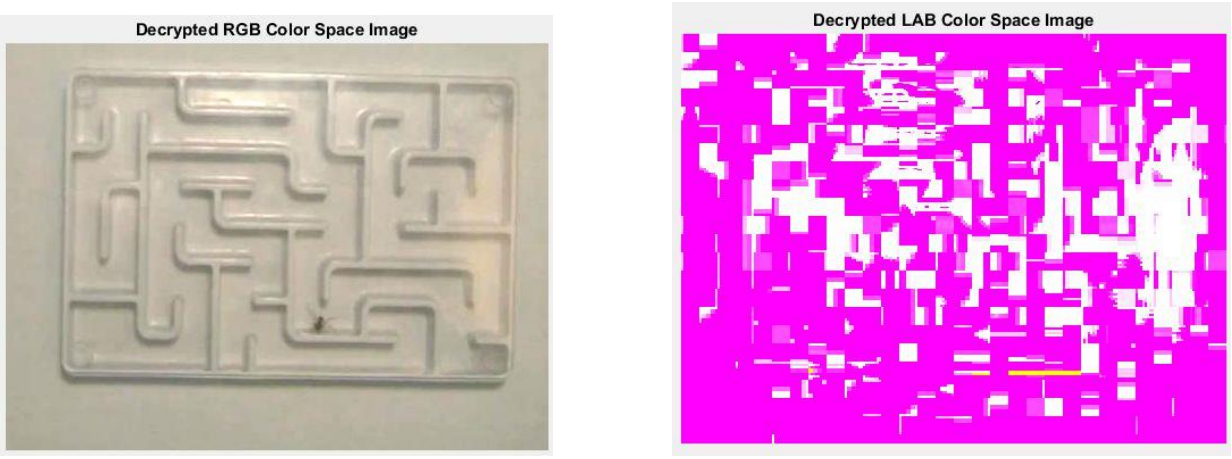


Fig. 3 Decrypted image in RGB vs LAB

In the fig 1, it shows the comparison result of a single frame in both RGB and LAB colour space. From the figure it can be easily shown that one can easily find the data information in RGB by viewing it. But in LAB colour space one cannot predict the actual output. That is the reason to use the LAB colour space.

In the same way fig 2 represents the encrypted image for the same original image with RGB and Lab colour space. Also in Fig 3 decryption of original image in both of the colour space has shown.

In the figure only the single frame of the video has shown, the actual video with encryption and decryption has been shown as follows:

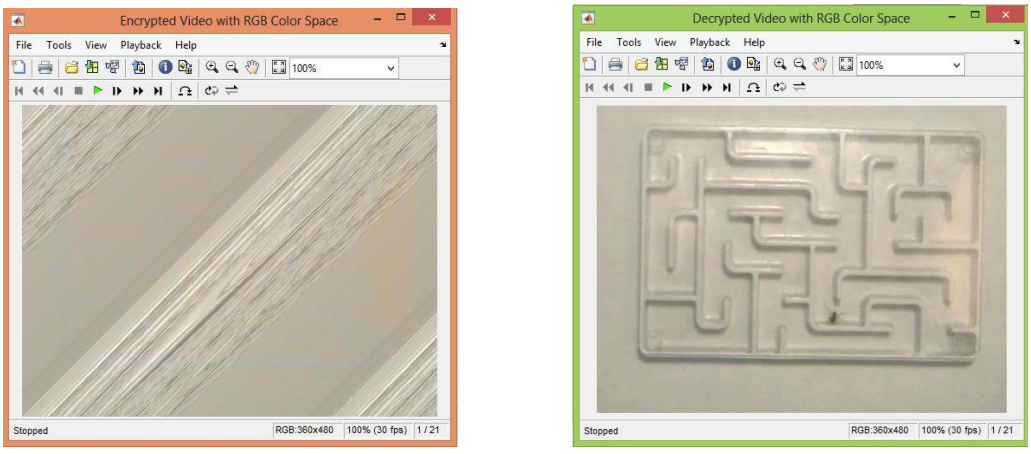


Fig 4 Encrypted and Decrypted Video in RGB

Fig 4 shows the encrypted as well as decrypted video in the figure. Which shows that encrypted RGB shows totally chaotic video, one can't get the information without having the true logic key.

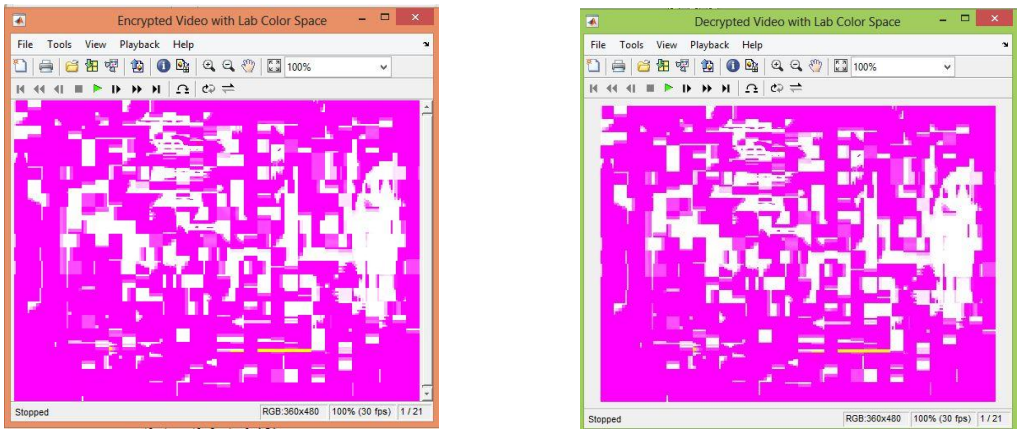
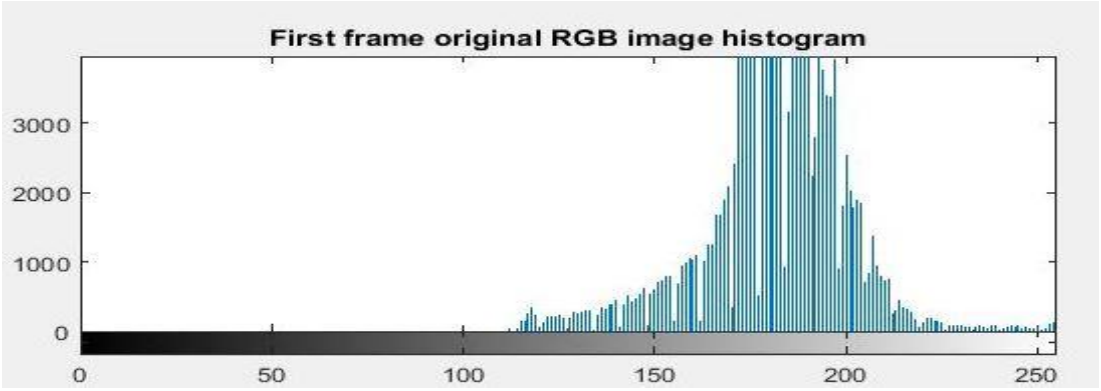
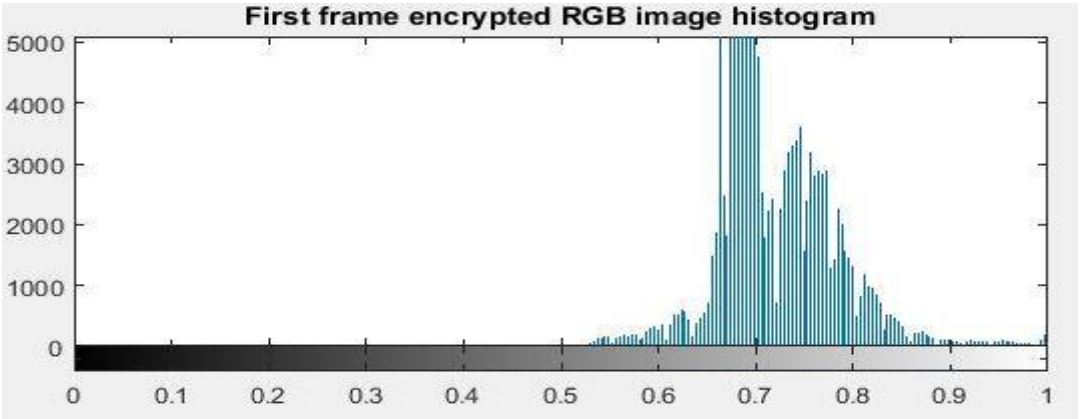


Fig 5 Encrypted and Decrypted video in LAB

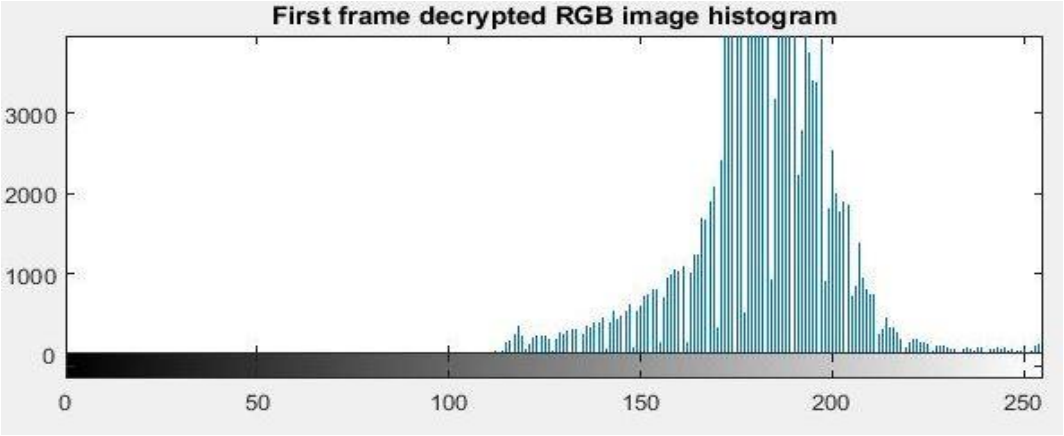
IV. STATISTICAL ANALYSIS



(a)



(b)



(c)

Fig 6 histogram for (a)Original image (b)Encrypted image (c)Decrypted image

Here by in figure 6, histograms of the original image have been shown. There is quite simple and easy correlation between all of them. Thus while from all above histograms, analyses can be done that histogram of both original and decrypted image will be approximately similar.

V. CONCLUSION

The paper goes for building up a secure algorithm for video encryption. The encryption algorithm utilizes two ideas, i.e., confusion and diffusion stage among the pixels of the grey scale image. Bit level stage not just changes the areas of the image pixels, additionally adjusts their qualities. Such an outline can improve the randomness. In this algorithm the pixel position is changed by randomly of the disorderly components, which is determined by contrasting sorted and unsorted disorganized components created from confusion map. This algorithm totally evacuates the layouts of the scrambled images, obscures the conveyance attributes of RGB-level lattices. The simulation results for image demonstrate that the proposed algorithm has extraordinary execution as far as sensitivity, velocity, and security. To finish up, all the encryption schemes are valuable for ongoing image encryption and every scheme is remarkable in its own specific manner which is proper for various applications.

References

[1] Minal Govind Avasare , Vishakha Vivek Kelkar.” Image Encryption using Chaos Theory.” 2015 International Conference on Communication, Information & Computing Technology (ICCICT), Jan. 16-17, Mumbai, India
[2] M. Abomhara, Omar Zakaria, Othman O. Khalifa. “An overview of vide encryption technique.” International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010 1793-8201.
[3] Nidhi Sethi , Sandip Vijay. A hybrid Cryptosystem for Image using Chaotic Mapping. ISSN: 1694-2108 | Vol. 5, No. 1. SEPTEMBER 2013
[4] Manjunath Prasad, K.L.Sudha, “Chaos Image Encryption using Pixel Shuffling.” D.C. Wyld, et al. (Eds): CCSEA 2011, CS & IT 02, pp. 169–179, 2011. DOI: 10.5121/csit.2011.1217
[5] Prachi Junwale , R. Manasa Annapurna, G.Sobha, “A Review on Image Encryption Technique based on Hyper Image Encryption Algorithm.” International Journal of Advanced Research in Computer Science and Software Engineering 3(11), November - 2013, pp. 614-618
[6] G.J. Sullivan, J. Ohm,W.-J. Han, T.Wiegand, “Overview of the High Efficiency Video Coding (HEVC) standard,” IEEE Trans. Circuits Syst. Video Techn., vol. 22, no. 12, pp.1649-1668, Dec. 2012.
[7] ITU-T and ISO/IEC JCT-VC, “Infrastructure of audiovisual services-coding of moving video,” ITU-T Rec. H.265, Apr. 2013.