International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 03, Issue: 04 (JULY- AUGUST, 2017)

# Enhanced Security for Encrypted Image Transmission over Communication Network: A Review

**Alpana Sharma[1], Manisha Singh[2], Kamlesh Gupta[3]**
[1] Phd Scholar Department of CSE, [1,2]Amity University Gwalior, MP, India
[3]RJIT, BSF Academy Gwalior, MP, India
[1]profalpanasharma[AT]rediffmail.com, [2]msingh[AT]gwl.amity.edu, [3]kamlesh_rjitbsf[AT]yahoo.co.in

**Abstract: -** Today's world, communication network structure rapidly grows due to number of user interaction increases day by day. Data transmission over network is easier but security is measure concern, so that number of researcher emphasizes to concentrate and to resolve the issue of security under data exchanging from one terminal to other. Data is a form of text, image, video and audio etc. while those given data is transmitted over network, than number of different encryption standards are better for different data sets. I.e. for that text RSA, AES are better, image encryption chaotic map are more suitable similarly many more encryptions and vice versa data. In this paper we investigate about various image encryption techniques for privacy of image against unauthorized access. But they all are work against unauthorized access control so due to that reason in this paper we proposed a enhance defence mechanism to protect the communication network from not only unauthorized access, it's also defend through network attack i.e. black hole, gray-hole, packet dropping etc while data transmitted by communication link.

**Keywords:** Cryptography, Chaos Theory, Black hole attack, Gray Hole Attack, Dropping and capturing attack.

## I. INTRODUCTION

Cryptography is that the science of protective the privacy of information throughout communication under hostile conditions. Within the present era of information technology and proliferating computer network communications, cryptography assumes special importance. Cryptography is currently habitually wont to defend information that should be communicated and/or saved over long periods, to shield electronic fund transfers and classified communications. [16]

With the development and progress of science and technology, hiding the information has evolved furthermore and located its position as a strong tool so as to keep up the information. Nowadays, communication through communication system has magnified dramatically at completely different levels, therefore there's continuously the chance of eavesdropping and tampering by enemy or profiteering that threatens this information. The protection of image together of the most common exchangeable information is taken into thought with the progress of technology within the past decade to stop unauthorized access or packet dropping at network level. Therefore researchers are searching for how to hamper the rate of correlation between the pixels within the images. So, high correlation between the pixels of the images can ease guessing the original one [17]. There are several digital images are present in data communication system that being sent over computer networks. With the increasing growth of multimedia system applications i.e. audio, video and images, security is a very important aspect in data communication. There's one among the apparent ways in which to confirm security is Image encryption. this method is attempt to convert original image to a different image that is tough to know and to keeps the image confidential between users, in different word, it's necessary that while not decryption key nobody will access the content. Image encryption has applications in internet communication, multimedia system systems, medical imaging, telemedicine, military communication etc. For privacy protection of digital images, encrypted records is a significant technological capability in cooperative information management. [4]

Image transmission security is another aspect of security vision that shield from routing or information drop attack whereas the data carry in channel and transfer over communication network. In this paper we tend to survey regarding numerous image encryption techniques and its impact we also study about network attack and its protection mechanism and based on that we proposed a strategy that offer application layer and routing layer security with the help of encryption and defender node deployment within the network. Our survey paper describes chaos primarily based cryptography, chaotic systems, literature survey, proposed work, conclusion and future scope of proposal.

## II. CHAOS BASED CRYPTOGRAPHY

Chaos primarily based cryptography continues to be in its infancy and will not have actual correspondence to ideas and notions of traditional crypto logic and cryptanalytic approaches. In such a scenario, our approach has been to reinforce security of the theme by providing larger key space, protection against reconstruction dynamics and resistance from statistical attack. Proving the safety of encryption supported chaos is still an open topic as a result of one cannot use the analytical strategies of classical cryptography that are supported number theoretic concepts or hardness of separate logarithmic problem [16].

A chaotic dynamical system could be a deterministic system that exhibits seemingly random behaviour as a results of its sensitive dependence on its initial conditions and might never be given with infinite precision. The chaotic system behaviour is unpredictable; thereby it resembles noise. The close relationship between cryptography and chaos makes a chaos based mostly crypto logic algorithmic rule a natural candidate for secure communication and cryptography. Crypto logic algorithms and chaotic maps have similar properties like sensitivity to changes within the initial conditions and management parameters, pseudorandom behaviour and unstable periodic orbits with long periods. The essential principle of image encryption exploitation chaos relies on the flexibility of some dynamic systems to provide sequence of numbers that are random in nature. Messages are encrypted victimization these sequences [18]. Because of the pseudorandom behaviour, the output of the system appears random within the attacker's read whereas it appears as defined within the receiver's view and decryption is feasible [19]. A very important difference between cryptography and chaos maps is that encryption transformations are defined on finite sets whereas chaos maps have that means only for real numbers [18]. Every chaos map has parameters that are similar to encryption key in cryptography.

Chaos is one among the possible behaviours related to evolution of a nonlinear physical system and occurs for specific values of system parameters. The invention of this apparently random behaviour succeeding out of deterministic systems clad to be quite revolutionary resulting in several problems interconnecting stability theory, new geometrical features and new signatures characterising dynamical performances [16].

Rucha R. Raut ET. al. has been proposed "An Enhanced Technique for Secure Image Transmission Via Visual Cryptography and Secret Fragment Visible Mosaic Images" [1] during this paper a brand new sort of pc art image known as secret fragment visible mosaic image is planned that transforms mechanically a given large-volume secret image into a thus known as secret fragment visible mosaic image. The mosaic image, that appearance the same as a willy-nilly designated target image and will be used as a camouflage of the key image, is yielded by dividing the key image into fragments. The knowledge needed for sick the key image is embedded into the created mosaic image by a lossless data concealment theme employing a key. Shamir secret sharing formula plays a vital role during this project. Shamir's secret sharing is a formula that divides a secret into shares. For secret writing of secret image Shamir secret writing technique is employed and for secret writing method Shamir secret writing formula is employed. Secret will be recovered by combining sure numbers of shares. A further live to boost the embedded knowledge security is additionally planned.

Ali Soleymani ET. Al. has a title "A Survey on Principal Aspects of Secure Image Transmission" [2] this paper may be a review on the aspects and approaches of style a picture cryptosystem. During this paper they outline in a very general introduction for cryptography and pictures secret writing and followed by completely different techniques in image secret writing and connected works for every technique surveyed. Finally, general security analysis ways for encrypted pictures area unit mentioned.

Asmaa Sabet Anwar ET. Al. proposed "Improving the security of images transmission" [3] they use a secret writing theme for inscribe medical image and analyze the performance beneath transmission over network of necessary medical pictures. During this paper they identifies the approved person will rewrite this medical image and may get the initial image. The possession of those medical pictures is extremely necessary to enhance. They will determine the possession of any medical image by mistreatment watermark associated with the owner of this medical image. They used name of the patient and serial variety. Capture the ear image of the owner then extract options from ear then inscribe those options then used it as watermark. The scale of the medical image is extremely effective purpose in transmission via web. As a result of their planned system used mixture of compression techniques applied on medical image before causing via web. To cut back run time and complexness of their planned system, they will use DWT to separates a picture into approximation image LL, metric capacity unit LH and HH.

Reshu Choudhary ET. Al. has a title to work "Secure Image Transmission and Evaluation of Image Encryption" [4] during this paper they present a formula for concealment a secret image within the least vital bits of a canopy image. They take exemplary pictures could also be colored or grey scale pictures. An elementary task in several image process applications is that the visual assessment of a distorted image. There are units several measures for examining image quality, like the mean structural similarity, mean absolute error, Mean sq. Error (MSE), and Peak S/N (PSNR). They computed by averaging the square intensity variations of distorted and original image pixels, beside the connected amount of the PSNR. Their experimental results show that very same size pictures area unit expeditiously encrypted with reliable PSNR as compared with completely different size pictures. Their planned system not solely shows the potency out of sight the attributes however conjointly provides higher cowl image choice.

Pooja Mishra ET. Al. has been proposed "Highly Secure Method for Image Transmission Using Partition and Multi Encryption Technique" [5] during this paper; they're mistreatment multi secret writing technique. Here they mistreatment quite one secret writing

formula. At the start they apply segmentation method to divide the image in to two equal elements. This image elements area unit encrypted through secret writing formula. In secret writing for every image half they're mistreatment completely different secret writing key. Then add n bits to every image elements to spot it unambiguously. Secret writing keys area unit depends on extra bits. Once secret writing they're causing image elements through the network. At the receiver aspect first extract the extra bits then apply secret writing formula into the image elements with the assistance of applicable secret writing key.

Priya R Sankpal ET. al. [6] has been proposed "Image Encryption Using Chaotic Maps: A Survey" during this survey paper, the present chaos based mostly image secret writing schemes are mentioned and analyzed to validate their performance against differing types of attacks. To conclude, the entire secret writing themes area unit helpful for real time image secret writing and every scheme is exclusive in its own method that is acceptable for various applications. Security will be increased by having multiple chaotic maps for image secret writing. Conjointly there are units more chaotic maps that require to be explored. To call few we've got Duffling map, Horseshoe map, Ikeda map, Gauss map etc. therefore secret writing which will be referred as a scientific art that is ever dynamical and quick growing must always exhibit high rate of security.

G. A. Sathish kumar et. al. [7] has title "image encryption based on diffusion and multiple chaotic maps" This paper presents a brand new formula for the image encryption/decryption theme. This paper is dedicated to give a secured image secret writing technique mistreatment multiple chaotic based mostly circular mapping. During this paper, first, a combine of sub keys is given by mistreatment chaotic supplying maps. Second, the image is encrypted mistreatment supplying map sub key and in its transformation results in diffusion method. Third, sub keys area unit generated by four completely different chaotic maps. Supported the initial conditions, every map could manufacture numerous random numbers from numerous orbits of the maps.

Among those random numbers, a particular a specific a designated variety and from a selected orbit area unit selected as a key for the secret writing formula. Supported the key, a binary sequence is generated to manage the secret writing formula. The input image of 2-D is remodelled into a 1- D array by mistreatment 2 completely different scanning pattern (raster and Zigzag ) and so divided into numerous sub blocks. Then the position permutation and worth permutation is applied to every binary matrix supported multiple chaos maps. Finally the receiver uses an equivalent sub keys to rewrite the encrypted pictures. The salient options of the planned image secret writing technique area unit loss-less, smart peak signal–to noise quantitative relation (PSNR), regular key secret writing, less cross correlation, terribly sizable amount of secret keys, and key-dependent pel worth replacement.

Rezvaneh Babazade Gorji et. al.[8] "A new image encryption method using chaotic map" This paper presents a brand new image secret writing technique supported supplying and Tent chaotic maps and permutation-diffusion design, in which, chaotic maps can amendment the pixels of the plain-image to inscribe that. Finally, the encrypted images are decrypted to remake the plain-image.

Vijayakumar. P et. al. present a paper "Enhancing the Secure Data Transmission for Routing Attacks in MANET" [9] during this paper they planned a risk aware resolution for mitigating MANET routing attacks .mainly their approach contemplate the secure knowledge transmission against the routing attacks. It's supported the Dempster-Shafer theory of proof with notion of importance issue. This identifies the routing attacks further as finding attacked node whereas transmission knowledge. Mistreatment each the table recovery and packet marking knowledge to be sent in less time and secured method. It'll results in finding the network risk.

Rajani Muraleedharan et. al. present a title of "Detecting Sybil Attacks in Image Sensor Network Using Cognitive Intelligence" [10] during this paper, a picture detector Network (ISN) beneath Sybil attack is analyzed and a completely unique detection mechanism mistreatment hypothesis testing with Cognitive Intelligence is planned. The performance of the appliance alone depends on accurately characteristic pictures beneath harsh environmental conditions. Since the network changes over time, a psychological feature formula, Swarm intelligence (SI) is employed in police investigation and re-routing the image co-efficient. The planned technique, doesn't need any extra hardware, therefore the survivability of the sensors is maintained, creating the appliance strong, value effective and energy economical.

Marianne Azer et. al. has been proposed "A Full Image of the Wormhole Attacks Towards Introducing Complex Wormhole Attacks in wireless Ad Hoc Networks" [11] during this paper, they involved of a very severe security attack that affects the unexpected networks routing protocols, and it's known as the whole attack. They imagine of whole attack as a two part method launched by one or many malicious nodes. Within the 1st part, these malicious nodes, known as whole nodes, attempt to lure legitimate nodes to send knowledge to different nodes via them. Within the second part, hole nodes might exploit the info in kind of ways that. They introducing the hole attack modes and categories, and purpose to its impact and threat on unexpected networks. They also analyze the wormhole attack modes from an attacker's perspective and suggest new improvements to this type of attacks.

Rashmi Hegde et. al. has a title "Steganography in Ad Hoc Networks" [12] This paper may be a combined contribution to the sector of steganography and ad-hoc networks. numerous unexpected networks attacks area

unit studied, and steganography ways to assist fight them so as to grant a brand new approach to security in unexpected networks. The planned resolution attracts a lot of importance because it ensures 2 layers of security through secret asynchronous knowledge sharing through completely different methods beside mistreatment steganographic ideas.

Rakesh Kumar et. al. present a title "Secured Image Transmission Using a Novel Neural Network Approach and Secret Image Sharing Technique" [13 during this paper they combined each cryptography and steganography techniques. This provides the upper level of secure system within which the key info will be transferred over any unsecured communicating and to beat the threat of intrusion. Their work aims at secure image transmission wherever a random secret writing formula is employed to inscribe completely different shares of stego image that is formed once a secret image and also the cowl image area unit embedded along, and produces shares employing a secret sharing technique. At the receiving finish, secret writing of the encrypted shares area unit done mistreatment a man-made neural network and therefore eliminating the requirement of key exchange before the transmission of knowledge that may be a requirement for many of the overall secret writing formula. Artificial neural network is employed to supply high security of knowledge and to supply distortion less decrypted pictures. The process is employed to reconstruct the key image from the decrypted pictures. Peak signal to noise quantitative relation, structure similarity and mean sq. error area unit wont to analyze the standard of stego pictures. Their simulation results show that the key is reconstructed while not loss and also the time taken for secret writing and secret writing is extremely less.

Ms. Prakruti Bisen et. al. present a title "An Approach For Secure Image Transmission " [14] ] during this paper, the secret writing ways (Symmetric key secret writing and uneven key encryption) area unit highlighted beside their examples. conjointly they need surveyed existing analysis on image secret writing in a very new approach mistreatment different techniques quite solely secret writing. These techniques were partial secret writing, chaos maps, public key and block transformation that applied to enhance and enhance the potency of a picture secret writing formula. Finally, they conferred secure approach for enhancing a lot of security of image whereas motion through networks.

Pooja Shelar et. al. present a title "A New Protected Image Transmission Idea via Secret-Splits-Visible Mosaic Images by Nearly Reversible Colour Transformations" [15] during this paper, a regular chaos based mostly image cipher with a 3D cat map-based abstraction bit-level permutation strategy is planned and compared with those recently planned bit-level permutation ways, the diffusion result of the new technique is superior because the bits area unit shuffled among completely different bit planes instead of inside an equivalent bit-plane. Moreover, the diffusion key stream extracted from hyper chaotic system is expounded to each the key key and also the plain image, which boosts the safety against known/chosen plaintext attack.

G. Chen, Y. Mao, and C. K. Chui [16], Author demonstrated that a variety of effective chaos-based image encryption schemes have been proposed. The everyday structure of those schemes has the permutation and also the diffusion stages performed or else. The confusion and diffusion result is alone contributed by the permutation and also the diffusion stage, severally. As a result, a lot of overall rounds than necessary area unit needed to attain a definite level of security. During this paper, they counsel to introduce sure diffusion result within the confusion stage by easy sequent add-and-shift operations. The aim is to cut back the employment of the time intense diffusion half in order that fewer overall rounds and therefore a shorter secret writing time are required.

L. H. Zhang, X. F. Liao, and X. B. Wang [17], First, for the resistance to differential attack and linear attack, they hints the rather smart datum properties of distinct exponential chaotic maps, In virtue of them, they designed a abstraction S-box, and then, then style a key theme for the resistance to datum attack and gray code attack. In fact, the theme will resist to the error perform attack (EFA) that be considered a really effective attack recently. Finally, Experimental and analytic results show that the theme is economical and extremely secure.

## III. PROPOSED WORK

Secure image transmission over communication is a big challenge, because user authentication not secure to hundred percentage of data transmission over communication medium. So our proposal is to secure the communication network while image data are transmitted over communication. While we transmit image data over communication medium than image is converting in the form of segments and that segmented data wrap-up with header of the transport layer and gives to below layer of routing layer and at the end while that data goes into the physical layer its convert in the form of pulse i.e. electrical, electromagnetic or infrared etc. (its depends on communication medium). That data transmit to the next hop and retrieve by the receiver node, but the above technique only for image transmission in unsecure manner. In this paper we focus to secure the image data transmission through encryption as well as network layer protection for reliable service to the end users. For that split the security technique into two module namely image encryption and transmission security, because before the our proposed work previous research paper's focus only the encryption of data and protect from un-authorized access and through the previous encryption mechanism we identifies that chaotic map provide very powerful security for image data against un-authorized access but they can't work for image transmission security infrastructure, than the our second module to prevent the data while image transmitted via communication medium under different intermediate nodes and number of routing attacks are presented i.e.

gray hole, black hole, vampire, dropping and capturing attack. That work provides transmission security as well as authorized access.

## IV. CONCLUSION AND FUTURE SCOPE

In this paper we study about how the image is securely transmitted via communication medium. From the literature reviews we found that Rucha R. Raut et. al applies visual cryptography technique for image transmission is used but routing security not measured. Asmaa Sabet Anwar et. al. encrypt the sensitive medical images via water marking methodology but that is also require some of extra enhancement of security so the un-authorized access are total blocked. Reshu Choudhary are secures the image transmission with the help of hiding the secret image with least significant bit and analyzed the PSNR, error rate, mean square error etc. and measure the quality of service of the network that helps to identification of attacker behaviours. Priya R Sankpal use the chaotic map technique and encrypt the image, chaotic map technique is more powerful for image encryption and attacker node easily decrypt because random pair of key are apply for encryption time. That work enhanced through the routing protection mechanism so our image encryption is powerful as compare to existing methodology. Paper also describe various routing attacks under mobile ad-hoc network and its protection methodology that work helps to provide how the communication network are protected via black hole, rushing and gray hole attacks, while the data transmission are done from sender to destination nodes. in this paper we also describe about outline of our proposed approach for image encryption as well as routing protection mechanism and provide reliable communication and transmission of secure image while nodes or terminals are work are router. In future proposed approach simulate through network simulator-2 and after that we compare our outcomes through existing encryption and image security techniques.

## REFERENCES

[1]. Rucha R. Raut, Prof. Komag B. Biwa “An Enhanced Technique for Secure Image Transmission via Visual Cryptography and Secret Fragment Visible Mosaic Images” IJSR, ISSN (Online): 2319-7064, Volume 4 Issue 4, April 2015.

[2]. Ali Soleymani, Zulkarnain Md Ali, and Md Jan Nordin “A Survey on Principal Aspects of Secure Image Transmission” International Scholarly and Scientific Research & Innovation, Vol: 6, No: 6, 2012.

[3]. Asmaa Sabet Anwar, Kareem Kamal A. Ghany, Hesham El. Mahdy “Improving the security of images transmission” IJBMIeH, Volume 3, No.4, June - July 2015.

[4]. Reshu Choudhary and Arun JB "Secure Image Transmission and Evaluation of Image Encryption" IJISET, Vol. 1 Issue 2, April 2014.

[5]. Pooja Mishra, Biju Thankachan "Highly Secure Method for Image Transmission Using Partition and Multi Encryption Technique" IJSR, ISSN: 2319-7064, Volume 2 Issue 7, July 2013.

[6]. Priya R Sankpal, P. A. Vijaya "Image Encryption Using Chaotic Maps: A Survey" IEEE, 978-0-7695-5100-5, DOI 10.1109/ICSIP.2014.80,2013.

[7]. G. A. Sathishkumar ,Dr. K. Bhoopathy bagan and Dr. N. Sriraam "image encryption based on diffusion and multiple chaotic maps" IJNSA,Vol.3, No.2, March 2011.

[8]. Rezvaneh Babazade Gorji, Mirsaeid Hosseini Shirvani, Farhad Ramezani Mooziraji "A new image encryption method using chaotic map" JMEST, ISSN: 3159-0040, Vol. 2 Issue 2, February – 2015.

[9]. Vijayakumar. P, Tamizharasan. P "Enhancing the Secure Data Transmission for Routing Attacks in MANET" IJARCSSE, ISSN: 2277 128X, Volume 3, Issue 11, November 2013.

[10]. Rajani Muraleedharan, Yanjun Yan and Lisa Ann Osadciw "Detecting Sybil Attacks in Image Sensor Network Using Cognitive Intelligence" Syracuse University, Syracuse, NY- 13244-1240.

[11]. Marianne Azer, Sherif El-Kassas, Magdy El-Soudani "A Full Image of the Wormhole Attacks Towards Introducing Complex Wormhole Attacks in wireless Ad Hoc Networks" IJCSIS, Vol. 1, No. 1, May 2009

[12]. Rashmi Hegde, Dr. T H Sreenivas "Steganography in Ad Hoc Networks" IJCSIT, ISSN: 0975-9646, Vol. 6 (6), 2015.

[13]. Rakesh Kumar and Meenu Dhiman "Secured Image Transmission Using a Novel Neural Network Approach and Secret Image Sharing Technique" ijsip, Vol. 8, No. 1 (2015), pp. 161-192.

[14]. Ms. Prakruti Bisen, Prof. Dipak Wajgi "An Approach for Secure Image Transmission" IJERA, ISSN: 2248-9622, April 2014.

[15]. Pooja Shelar, Archana Chaugule "A New Protected Image Transmission Idea via Secret-Splits-Visible Mosaic Images by Nearly Reversible Colour Transformations "IJCA, ISSN: 0975-8887, Volume 135 – No.4, February 2016.

[16]. Q.V. Lawande, B. R. Ivan and S. D. Dhodapkar "chaos based cryptography: a new approach to secure communications" BARC News Letter, No. 258 July 2005.

[17]. Narendra Singh, Aloka Sinha, "Optical image encryption using fractional Fourier transform and chaos". Optics and lasers in engineering. Vol, 46. Issue 2, pages 117-123. February 2008

[18]. Alireza Jolfaei, Abdolrasoul Mirghadri,” An Image Encryption Approach using Chaos and Stream Cipher”, Journal of Theoretical and Applied Information Technology, pp 117 – 123.

[19]. Somaya Al-Maadeed, Afnan Al-Ali, and Turki Abdulla, a New Chaos-Based Image-Encryption and Compression Algorithm”, Hindawi Publishing Corporation, Journal of Electrical and Computer Engineering, Volume 2012.