COLOR CRYPTOGRAPHY USING SUBSTITUTION METHOD

A.SIVASANKARI[1],M.KAMARUNISHA[2],S.GOWRI[3]

Assistant professor, department of computer applications

Dhanalakshmi srinivasan college of arts and science for women perambalur

ABSTRACT

The dangers to data security are expanding at quickly. The best and general way to deal with counter such dangers is encryption. In Traditional encryption procedures replacement and rendering is utilized. In Substitution procedures plaintext is planned into figure text. In all conventional replacement methods plaintext characters, numbers and extraordinary images are subbed with another characters, numbers and uncommon images. In this new strategy an imaginative cryptographic replacement is proposed to produce a more grounded figure than the current replacement calculations. This technique centre around the replacement of characters, numbers and extraordinary images with shading blocks. This calculation of replacement depends on Play Color Cipher. This is an even framework which is executed by encryption of text by changing over it into colors. Each character of the plaintext is scrambled into a square of shading. Each character will be subbed by an alternate shading block. A tale strong content encryption strategy by utilizing Armstrong number, shading code, prime number and ASCII codes by utilizing replacement and stage procedure. In this encryption procedure 512-cycle size key is utilized for encryption. In replacement strategy message is changes into ASCII codes .In the proposed procedure irregular Armstrong number, prime number, shading code are created and key is scrambled by base-64 encoding for greater security. In the change cycle increase, expansion is performed on the information for encryption. The proposed approach deals with the symmetric encryption. The proposed method is then contrasted and the standard IDEA calculation. Result shows that the proposed method is hearty, quick and secure

KEYWORDS: Data security, IDEA, Text encryption, substitution, permutation.

INTRODUCTION

Data security is the wellbeing of data and limits the danger of presenting data to unapproved social affairs from uncover, change, and devastation of information. Cryptography is a strategy for putting away and leading information in a specific structure with the goal that lone those for whom it is future can peruse and handle it. The security of code text is absolutely needy two things: the intensity of the cryptographic calculation and the protection of the key. Numerous scientists have adjusted the current calculations to satisfy the need in the current market, yet the codes are powerless to assaults.

The new period of online media has prompted the inflow of enormous measure of information. This information which may appear to be unstable have an extraordinary spot in information security. With this monstrous information, which is expanding second by second, come a few dangers, which are of incredible worry to secure the uprightness and protection of the source creating this information. This is the place where encryption assumes job. Presently a day's numerous encryption calculations permit us to encode information. Agreeing. "Information security is something exceptionally significant and need of great importance". At the point when plain content is changed over into garbled structure that is called figure text, is known as the encryption cycle and the converse of this code text to plain content is known as the decoding cycle. In cryptography when same key is utilized for encryption and unscrambling, it is called symmetric cryptography and when two distinct keys utilized for encryption and decoding, and afterward it is called topsy-turvy cryptography. In the proposed system RGB shading code assumes significant job

Shading Coded Encryption is a method of actualizing a balanced framework for security reason. The even framework is actualized by encryption of text by changing over it into picture design. To diminish the size of the picture record, pressure calculations are to be executed at the encryption stage. The opposite cycle is utilized to produce at the objective framework to recuperate the information in the first configuration. A cryptographic replacement procedure called Color coded cryptography which changes the

"Play Color Cipher". This calculation modifies the plain content in different manners before it takes the state of code text. This is a balanced system which is executed by encryption of text by transforming it into shading blocks. Each character of the message is encoded into a square of shading. Each character will be subbed by another shading block

At the collectors side opposite technique is used to get the first content. Here, in our framework symmetric key cryptography has been used. Our framework will have uphold for different dialects. On an essential level, Translator perform direct replacement of words in a single language for words in another, improving yield by confining the degree of tolerable replacements.

Threats and vulnerabilities in existing systems

RSA is involved on the inappropriate development of two prime realities. Henceforth, number factorization is a grave threatening in blunder of RSA and at present various types of spells have recognized against RSA by cryptanalysis. Most spells appear to be the impact of misuse of the plan or malicious selection of boundaries. Replacement techniques like Caesar Cipher, Mono alphabetic Cipher, play simply Cipher and Poly alphabetic Ciphers are not sufficient since they are weedy to savage power spells.

RELATED WORKS

In [1] Ehsan Hasanzadeh, Mahdi Yaghoobi et al presents a novel shading picture encryption conspire dependent on fractals, replacement box and hyper confused dynamic is proposed. In the initial step, fractal pictures are created by Julia fractal set as keys. At that point, the replacement box is developed by Hilbert fractal, and the first picture pixels are supplanted with the estimations of the S-box. In the following stage, utilizing the Logistic guide, the area of the pixels is mixed to decrease their connection. In the accompanying, Chen hyper confused framework is utilized to change the pixels estimations of fractal pictures just as file creation to choose fractal pictures. At long last, every pixel of three unique picture layers with the comparing pixels in the three chose fractal pictures and the past scrambled pixel esteem are encoded with XOR activity. Both test results and security examinations demonstrated that the proposed strategy yields high encryption impact, bigger secure key space and is high delicate to the mystery key and the plain picture. What's more, the calculation could oppose against different normal assaults. The hyper-riotous frameworks show higher protection from programmer assaults given their intricate nature and more key space than the turbulent frameworks. Moreover, an effective encryption calculation needs a key space huge enough for opposing visually impaired and serious assaults by programmers.

In [2] Devyani Patil, Vishakha Nayak, Akshaya Sanghavi, Aparna Bannore et al presents The arising dangers to data security are expanding at a disturbing rate. The most compelling and general way to deal with counter such dangers is encryption. Customary encryption strategies use replacement and rendering. Replacement strategies map plaintext into figure text. In all customary replacement procedures, characters, numbers and uncommon images are subbed with different characters, numbers and unique images. In this paper, an imaginative cryptographic replacement strategy is proposed to create a more grounded figure than the current replacement calculations. This strategy accentuates on the replacement of characters, numbers and uncommon images with shading blocks. This calculation of replacement depends on Play Color Cipher. The cryptanalysis done on this will demonstrate that the code is solid. The security of code text is totally reliant on two things: the intensity of the cryptographic calculation and the privacy of the key. Gatecrasher exercises as of late have made a requirement for creating more grounded and safer calculations. In late past numerous specialists have adjusted the current calculations to satisfy the need in the current market, yet the codes are helpless against assaults.

In [3] Prof. K. Ravindra Babu, Dr .S.Udaya Kumar, Dr. A.Vinaya Babu, and Dr. Thirupathi Reddy et al presents The most powerful and general way to deal with countering the dangers to arrange/data security is encryption. Despite the fact that it is exceptionally legitimate, the cryptanalysts are extremely astute and they were working day and night to break the codes. To make a more grounded figure it is prescribed that to utilize: more grounded and convoluted encryption calculations, Keys with more number of pieces (Longer keys), bigger square size as contribution to measure, use confirmation and classification and secure transmission of keys. It is sure that, in the event that we follow all the referenced standards, can make a more grounded figure. With this we have the accompanying issues: It is a tedious cycle for both encryption and decoding, it is hard for the tomb analyzer to break down the issue. Additionally endures with the issues in the current framework. The

fundamental expectation of this paper is to introduce an inventive cryptographic Substitution technique, can produce more grounded figure then the current replacement calculations. We are certain that idea is new and the cryptanalysis did on this will demonstrate that the code is solid.

In [4] Dr. D. Devakumari et al presents Transmission of information between the clients in the organization is a significant part of today, client of the organization needs to divide their data among different clients of made sure about information transmission. They were numerous method of exchange o information were done, yet made sure about degree of information exchange is a significant perspective what everybody needs. Mystery information transmission is as yet serious issue in organization. Implanting the mystery data is an overhauling innovation for sharing mystery information, installing measure cryptography strategy assumes a key job. Compelling installing of mystery information by utilizing visual cryptography helps a ton for mystery information transmission. This paper gives the study of different cryptographic strategies and its viability for secure transmission over organization. Visual cryptography plot is a mystery sharing of mystery picture shares which includes partitioning the mystery picture into number of offers and a specific number of offers are sent over the organization. The unscrambling cycle includes stacking of the offers to get the mystery picture. The primary preferred position of visual cryptography plot is that various qualified offers can recuperate the mystery picture with no cryptographic information, figuring and calculation gadgets

In [5] Aqeel Ur Rehman, Amnah Firdous, Salman Iqbal, Zahid Abbas et al presents An imaginative strategy proposed for scrambling shading pictures is contained one-time keys and bedlam hypothesis utilizing a particular idea of rotor machine. The oddity of this plan is that the lines and segments of 2-dimensional pictures are changed over into round article called rotor and can be pivoted at 360 degrees in clockwise or against clockwise course. The pivot will change the current rotor into new one and can be utilized in replacement cycle of plain picture. This cycle can be rehashed times and each time another rotor is made just by a straightforward revolution. The revolution is acted as far as pixels so level of point is changed over into number of pixels. Utilizing this technique, same item with new face is utilized for encryption. The pixels of shading picture are permuted utilizing the arranged list of calculated succession. At that point, three pseudo-arbitrary pictures are made from Piecewise Linear Chaotic Map (PWLCM). For replacement, both the permuted shading channels and pseudo-irregular pictures are changed into rotors. The point is gotten from Chen riotous framework. The one-time keys are for riotous guides are created by utilizing 512-bits hash of plain picture. The recreated results show that the proposed framework has high caliber of results and requires just single round of encryption to accomplish high encryption alongside high strength against the transmission commotions.

PROPOSED SYSTEM

A cryptographic replacement strategy is proposed which alters the "Play Color Cipher" that is called as Color coded cryptography. This framework depends on symmetric encryption which is executed by scrambling text into shading picture. Each character of the message is encoded into a square of shading. Each character will be subbed by an alternate shading block. The opposite cycle is utilized to create the first content from shading block at the beneficiary side. The client enters a message which is the plaintext sender side. A channel should be browsed the three shading channels for example red, green and blue (RGB). The client should indicate the qualities for the R, G and B channels between the reaches 0-255. Additionally a square size of shading block should be determined. All the characters of the content are then changed over to shading blocks framed by joining the estimations of R, G and B channels. In present work a book encryption method is proposed. Framework engineering of the replacement and change strategy in the proposed text encryption method has been portrayed. In present work sender and recipient keep an information base to store all data about key and information. Encryption is finished by the RBG shading codes, ASCII codes, Armstrong numbers and prime numbers. In this plan, 512-bit size key is utilized. The key likewise scrambled by base-64 encoding. After encryption of key the replacement cycle begins. In the replacement cycle the message is changed into its ASCII codes. In the stage cycle three irregular Armstrong number, one prime number and three ASCII numbers are produces and the encryption is finished by duplicating and adding of these numbers

Asymmetric cryptography

In Asymmetric cryptography two keys are utilized for encryption and decoding one is public key and other is private key. Public key is known by everybody except the private key is known simply by the beneficiary to decode the message. Strength of the PKC is relies upon that how the general population and private keys are produced. Model – RSA calculation

Secret key cryptography or Symmetric cryptography

In Secret key cryptography just a solitary is utilized for both encryption and unscrambling measure. In this sort the key is shared by both sender and recipient .This kind of framework are quick and straightforward. Both sender and recipient should utilize a safe line to communicate the key. At the point when an individual P needs to impart to individual Q they need a key for safely correspondence. It is important to trade key or key circulation. Such a huge number and Q trade the key and afterward communicates message. Model AES calculation, DSA calculation .The speed of encryption and decoding is extremely quick.

SYSTEM ARCHITECTURE

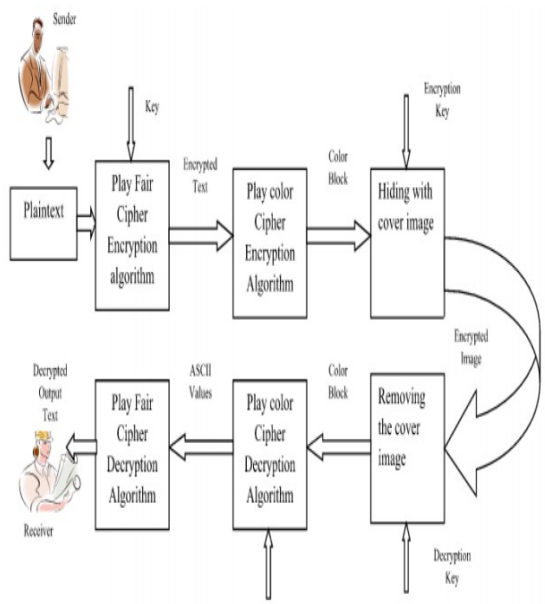

Fig system Architecture

ENCRYPTION

First acknowledge the information text and the key. Encode the content utilizing play reasonable code. Separate the scrambled content into singular characters .Find the ASCII estimation of each character (say x).Then discovers the situation of each character (say y). Add position worth and ASCII of each character (for example x + y=z).Then in the shading channels R, G, B the estimation of z is relegated to any of the channel, staying two will be inbuilt. At that point add the estimations of R, G, B to create a tone, which will be relegated to the particular character .Now the content will be changed over into shading blocks. The shading blocks are concealed utilizing cover picture.

DECRYPTION

The got cover picture is isolated into picture and shading blocks .The isolated shading block is splitted into singular shading block .Get the estimation of individual shading hinder and take away the key from that esteem. Discover the ASCII estimation of each character (say x). At that point discover the situation of each character (say y).Subtract position worth and ASCII of each character to get a scrambled content. Utilizing play reasonable code calculation, the scrambled content is decoded .The first content is acquired.

PROPOSED PROCESS

Substitution process

In replacement measure the characters of the message are changed over into its ASCII codes.

Base-64 encoding of key

In this cycle the base-64 encoding is performed on the 512-bit key. Base-64 guides all the double characters into a few standard ASCII letters and numbers and accentuation so it is utilized for safer and powerful transmission of message. Right off the bat the characters are changed over into its ASCII codes, after that the ASCII codes are changed over into base 2.

Permutation process

In the stage cycle irregular Armstrong number, prime number and ASCII numbers are produced and encryption of the message done.

The proposed Methodology

Calculation In the proposed calculation right off the bat 512-digit size key is creates. The encryption is totally relies upon the key. In the proposed calculation 3 arbitrary Armstrong number, 3 ASCII number and 1 prime number are created. The proposed calculation comprises of two cycle – replacement and stage.

Input: plain text X with secret key

Key size: 512-bit

Output: encrypted text

Begin

Procedure: substitution

- Get plain text (X)
- Transforms the plain text message into ASCII code
- Colour is selects and than the RGB value for this selected colour is fetch.
- Key is converted into base-64 encoding.

Procedure: permutation

1. Three random Armstrong numbers are multiplied by 3 ASCII numbers and addition into matrix A

2. RGB colour code is add into the result of matrix A and store into matrix B .

3. Now prime number is multiplied by the matrix B and result store into matrix C .

4. The matrix C is multiply by the message ASCII and store into matrix D

5. For encryption key is multiply by the matrix D and it is the encrypted text.

End

CRYPTANALYSIS

Considering the utilization of Login verification framework which utilizes the proposed cryptographic framework, the length of the key, which is a numerical capacity of timestamp (put away at the hour of enrolment) and client's date of birth, is a decimal number with limit of 28 digits. The key can be any mix of 0 to 9 numbers. In this way, the most extreme number of keys can be (10)28. In this manner, on the off chance that we perform one encryption for each miniature second it takes

$$\frac{10^{28}X10^{-3}}{365X24X60X60} = 3.17 \text{ X } 10^{17} \text{ years}$$

For shading replacement, just 3 boundaries (RGB) have been utilized where, each channel has a shading conceal scope of 0-255. Greatest number of shading mixes is 1,67,77,216 in decimal. It will be tiring to evaluate every conceivable blend. Subsequently it is protected to infer that the savage power assault is beyond the realm of imagination. Additionally, there are 18 Decillions of tones in the PC world. In this manner, if man in the centre, known plain content, known code text assaults is thought of, it won't be conceivable to figure or decode the plain content just by acquiring the shading picture.

APPLICATION

This game plan of concealing cryptography can be used for approval of login structures. During the selection system, the new customer will enter his own nuances and the mystery word. The mystery key is then mixed into a concealing coded picture using the proposed concealing replacement computation. The image is then taken care of at the worker. At the hour of login, the customer enters the username and mystery key. Taking into account the username, relating image of the mystery key is recuperated from worker, decoded and changed over to content. This substance is then planned with the mystery expression entered by the customer. If it facilitates, the customer viably signs in. The key for encryption and unscrambling can be established on the boundaries of the individual nuances entered by the customer. Mathematical limits performed on the timestamp of enrolment and client's date of birth can create a key

RESULT AND DISCUSSION

The usage of the proposed calculation has been acted in PHP. The usage is acted in c# language and the information base is makes on my SQL worker to store all data. The blend of replacement and stage makes it powerful. The security of the proposed text encryption calculation is tried.

(1) Scalability = Scalability defines on the basis of performance and memory required by the encryption algorithm. Memory required depends on number of variable and functions executed by the algorithm.

IDEA Algorithm = good performance and required less memory Proposed Algorithm = less memory , performance good but not better than IDEA.

(2) Security level = In proposed algorithm we used 512-bit size key and due to 512-key proposed system is more secure. Proposed algorithm is secured by brute-force and biclique attack.

(3) Avalanche effect= Avalanche effect is defined as the change in either 1 bit of plain text or key produce significant change in cipher text. IDEA algorithms and proposed algorithm are affected when changes in plain text or key.

(4) Computation time = Computation time is the time taken by the algorithm to perform the encryption of the text or image

Figure shows the computation time of the IDEA and proposed algorithm for over 650kb file size. Figure shows that average computation time in the range of 0.2sec to 2.2sec for proposed algorithm and for IDEA algorithm the computation time in the range of 0.7sec to 2.5sec. So we conclude that the time taken by proposed algorithm is slightly minimum in comparison to IDEA algorithm.

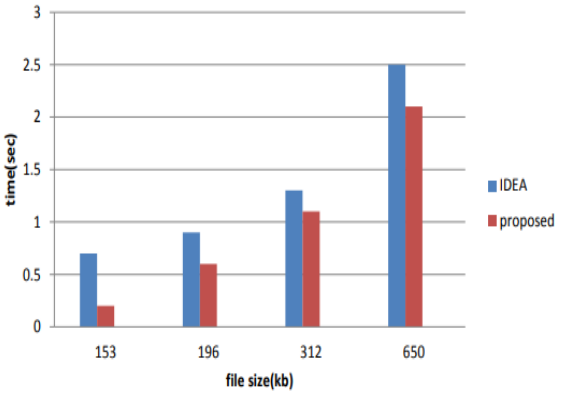

Figure 2: performance comparison of proposed algorithm with IDEA with respect to computation time

Encryption Throughput = Encryption throughput describes that how many unit of information are processed in given amount of time.

Encryption throughput = sum of input files/sum of encryption time (kb/sec)

Algorithm	Throughput(kb/sec)
IDEA	243.59
Proposed	327.5

Figure shows the throughput of IDEA and proposed algorithm. Figure shows that the throughput of IDEA is in the range of 0kb/sec to 250kb/sec and the throughput of proposed algorithm is in the range of 0kb/sec to 350kb/sec, which is more than IDEA throughput.

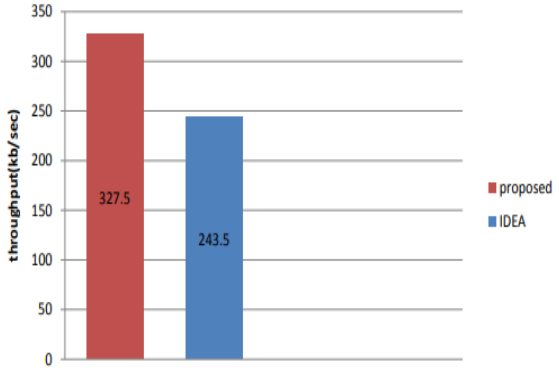

Figure 3: performance comparison of proposed algorithm with IDEA with respect to Throughput

(6) Encryption Rate = Encryption rate defined as the number of bytes encrypted per unit time. Algorithm that is high encryption rate is more secure compared to other algorithm.

Encryption rate = file size/encryption time

File size (kb)	Time(IDEA) sec	Time(proposed) Sec	Enc rate(IDEA) Kb/sec	Enc rate(proposed)kb/sec
153	0.7	0.2	218.57	765
196	0.9	0.6	217.77	326.66
312	1.3	1.1	240	283.63
650	2.5	2.1	260	309.52

Table 3: Encryption rate of IDEA and proposed algorithm

Parameters	IDEA	Proposed
Key size	128	512
Power consumption	Low	Low
Attack	Crack by brute force attack	More robust due to 512-bit key size
Key used	No encryption	Encrypted key
Encryption	Fast	Faster than IDAE
Block size	64	Depends on key and plain text

Table 4: Comparison between IDEA and proposed algorithm

CONCLUSION

The present standard cryptographic techniques are dependent upon an assortment of assaults. A creative methodology introduced and executed in this paper makes data secure by shading replacement. In future, the figures, tables, pictures, and so forth can be remembered for the plaintext for transformation and henceforth the extent of the calculation can be expanded. It built an encryption calculation which used to make sure about the information from unapproved individual .This paper present a calculation which is secure, proficient and strong. Results show that encryption of huge document by the proposed framework was safer on the grounds that numbers are haphazardly created and shading code utilized for verification just as encryption too. Thus we effectively built and investigated record transmission model utilizing encryption calculation.

REFERENCE

[1] S. Pavithra Deepa, S. Kannimuthu, V. Keerthika, February, 2011 “Security Using Colors and Armstrong Numbers” Kongu Engineering College, Perundurai, Erode, Tamilnadu, India.17 & 18.pp.157-160.

[2] Belose, S., Malekar, M., & Dharmawat, G. 2012. Data Security Using Armstrong Numbers Undergraduate Academic Research Journal (UARJ),volume 1,pp. 80-83.

[3] Saoji, S. A., Agarwal, N. B., Bokil, M. B., & Gosavi, A. V. 2013. Securing emails in XML format using colors and Armstrong numbers. International Journal of Scientific & Engineering Research (ISSN), 2229-5518

[4] Vanathi, R., Dhanam, L., Senthilnathan, K. R., & Vinu, M. S. 2013. Secured and Reliable Data Transmission Using Lychrel Numbers RGB Colors and One Time Password.

[5] .Vaidya, M., Bansod, V., & Manwar, M. 2014. A Review on Cryptography Using Armstrong Numbers and Colors. [6] .Gurav, N., & Singh, P. A Survey on Security Mechanism using Colors and Armstrong Numbers.

[7] . Kumar, A., Sinha, P., & Gupta, T. Steganography For Secure Message Passing. Using Armstrong Number And Color Code.

[8] Bellovin, S. M., & Merritt, M. 1992, May. Encrypted key exchange: Password- based protocols secure against dictionary attacks. In Research in Security and Privacy, 1992. Proceedings., 1992 IEEE Computer Society Symposon, pp. 72-84.

[9] 9.Blum,M., & Goldwasser, S. 1984, August. An efficient probabilistic publickey encryption scheme which hides all partial information. In Workshop on the Theory and Application of Cryptographic Techniques pp. 289-299.

[10] Needham, R. M., & Schroeder, M. D. Using encryption for authentication in large networks of computers Communications of the ACM,

[11] Renaud, “Evaluating authentication mechanisms,” in Security and Usability: Designing Secure Systems That People Can Use, L. Cranor and S. Garfinkel, Eds.O’Reilly Media, 2005, ch. 6, pp. 103–128.

[12] Jain, L. Hong, and S. Pankanti,2000. "Biometric identification," Communications of the ACM, vol. 33, pp. 168-176.

[13] Burke, J., McDonald, J., & Austin, T., Architectural support for fast symmetric-key cryptography, Independent Component Analysis: A Tutorial Introduction. MIT Press, Cambridge, MA (2004).

[14] Lavanya Reddy L,K.Alluraiah , August 2013: Enhanced Cued Click Point(ECCP) Method for “Graphical Password Authentication” International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 8.

[15] Chavan Satish, Lokhande Yogesh, Shinde Pravin, “Secure Email using Colors and Armstrong Numbers over web services”, International Journal of Research in Computer Engineering and Information Technology VOLUME 1 No. 2.