Chapter 9

Performance Analysis, Conclusion and Future Scope

9.1. Overview

New Ciphering protocols which are considered as 'building blocks' based on user authentication, text encryption and image encryption have been implemented and integrated together to generate 'security toolkit'. Performance of each of this implemented independent protocols has been measured based on the comparison with other existing standard algorithms like AES, Triple DES, Serpent, Blowfish, Twofish in chapter 5 and chapter 6. Comparisons of performances between the implemented protocols have been carried out in this chapter based on different standard parameters applicable to their respective domains.

In this chapter, comparisons of performances for user authentication building blocks, text encryption building blocks and image encryption building blocks have been accessed based on standard parameters like security over cryptographic attacks, chi-square value, PSNR, etc. Summary of research and future scope of work are also included in this chapter.

In this chapter, the performance analysis of building blocks and conclusions in section 9.2, a summary of research in section 9.3, the future scope of work in section 9.4 have been discussed.

9.2. Performance Analysis of Building Blocks and conclusions

Three 'building blocks' namely user authentication building blocks, text encryption building blocks and image encryption building blocks have been implemented in this work. Security over web attacks, CAPTCHA or OTP generation time and user authentication validation time are considered as standard parameters for user authentication building blocks. For text encryption building blocks, encryption time, chi-square value and degree of freedom value are taken for consideration as

performance assessment parameters. SSIM, PSNR, BER, Universal Image Quality Index (Q-INDEX), Correlation Coefficient, encryption time are considered for performance measurement. Detailed performance analyses for each of the building blocks are carried out in the next section.

A. Performance Analysis of User Authentication Building Blocks

Introducing of recognition and sequencing of representative CAPTCHA images based on user personal information has increased the security compared to existing CAPTCHA schemes. Implementation of multiple security layers based OTP schemes provides great security over existing OTP schemes where random selection of values, distribution of OTPs through mail and SMS, generation of separate OTPs for authentication and distribution, OTP extracted secret value based authentication are implemented in an intelligent manner. Table 9.1 and Figure 9.1 represent the percentage of security provided by the implemented CAPTCHA and OTP schemes over different web attacks where NIOTP scheme is more secure compared to SVROTP scheme and CCPUL scheme.

Table 9.1: Security Measurement of CCUPL, SVROTP, NIOTP Schemes over Cryptography Attacks

Type of Attacks	**Number of Login Attempts by Fake Users**	**Measurement of Security over Unauthorized Access (in percentage)**		
		CCUPL Scheme	**SVROTP Scheme**	**NIOTP Scheme**
Brute Force Attack	75	84%	86%	89%
Dictionary Attack	68	87%	89%	91%
Key Logger Attack	70	81%	88%	86%
Man in the Middle Attack	64	79%	82%	87%
Phising Attacks, Physical Access to Phone,Mobile Phone Trojans	65	73%	84%	90%

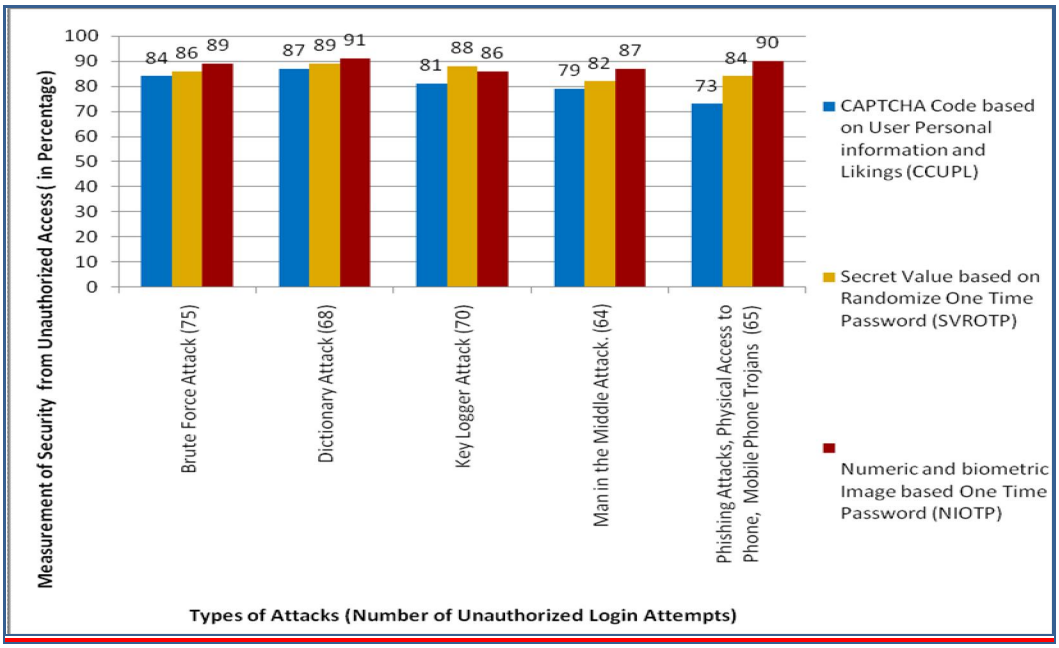

Figure 9.1 Graphical Representation of Security Measurement of CCUPL, SVROTP and NIOTP Schemes over Authentication Attacks

CAPTCHA and OTP generation time and user authentication validation time needed for implemented CAPTCHA and OTP schemes are represented in Table 9.2 and Figure 9.2 where CCUPL scheme takes the least time for CAPTCHA generation and user authentication validation compare to SVROTP scheme and NIOTP scheme.

Table 9.2: Requirement of CAPTCHA and OTP Generation Time and User Authentication Validation Time by CCUPL, SVROTP and NIOTP Schemes

Name of the CAPTCHA or OTP Scheme	**Time needed for CAPTCHA or OTP Generation at Server End (milliseconds)**	**Time needed for Validation of User Authentication at Server End (milliseconds)**
CCUPL Scheme	65881	5731
SVROTP Scheme	67315	7123
NIOTP Scheme	71894	8453

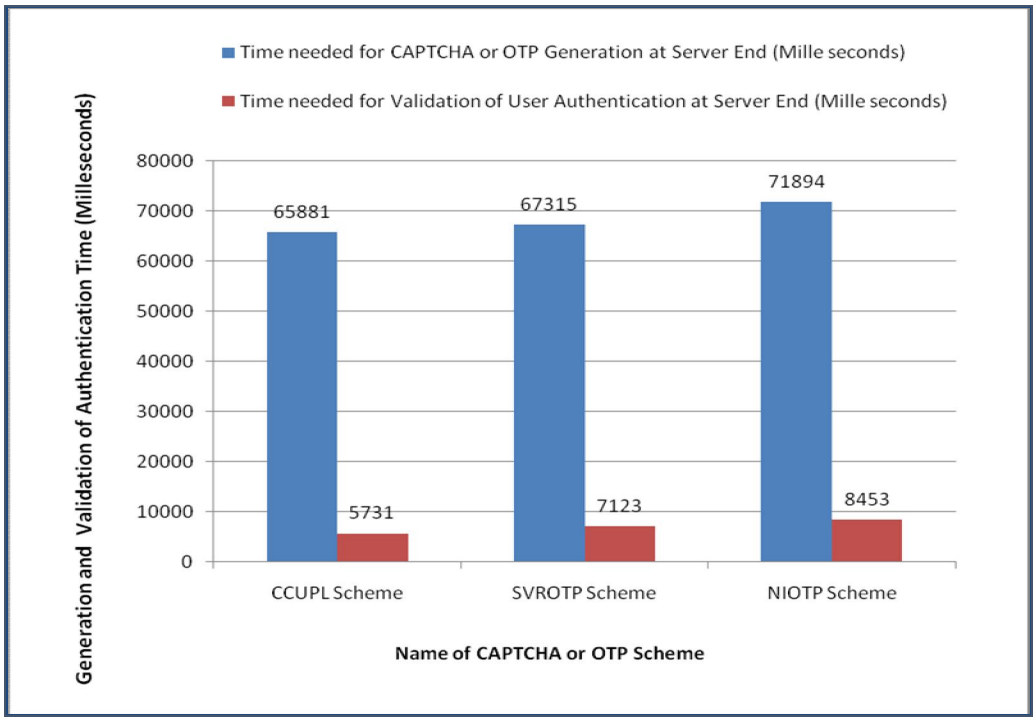

Figure 9.2: Graphical Representation of CAPTCHA and OTP Generation Time and User Authentication Validation Time by CCUPL, SVROTP and NIOTP Schemes

Table 9.3 represents the summarized performance assessment results of implemented CAPTCHA and OTP authentication schemes based on different parameters or criteria.

‘ê’ is applied as abbreviation where ‘ê’ represents average performance, ‘ê ê’ represent good performance, ‘ê ê ê’ represent very good performance and ‘ê ê ê ê’ represent extremely good performance. Performance measurement is carried out by the counting of ‘ê’.

From the table, it is shown that NIOTP scheme with multiple layers of security is the best performer compared to SVROTP and CCUPL scheme in respect of different performance assessment parameters.

Table 9.3: Summarized Performance Assessment Results of CCUPL, SVROTP and NIOTP Schemes

Name of Parameters / Criteria for Performance Assessment	Name of CAPTCHA or OTP based Scheme		
	CCUPL Scheme	**SVROTP Scheme**	**NIOTP Scheme**
Security over web attacks	ê ê	ê ê ê	ê ê ê ê
Time needed for CAPTCHA or OTP generation at server end (Milliseconds)	ê ê ê	ê ê ê	ê ê
Time needed for validation of user authentication at server end (Milliseconds)	ê ê ê ê	ê ê ê	ê ê ê
Numbers of security layers	ê ê	ê ê	ê ê ê ê

B. Performance Analysis for Text Encryption Building Blocks

Implementation of text encryption schemes based on the secret value derived from the private key rather than using the direct private key value have increased the security to a great extent. Applying of special numbers, alphabetic group, user defined cipher sequencing schemes has also increased the security for text encryption.

Encryption time for different files encrypted by the implemented text encryption schemes are represented in Table 9.4 where APCS and PAGO schemes are the best performers compared to other schemes as they take the least amount of encryption time rather than other schemes.

Table 9.4: Requirement of Encryption Time for Different Files by APCS, PAG, PAGO, MOEO, MOAV, MOZO and ACS Schemes

File size (Bytes)	APCS Scheme (milliseconds)	PAG Scheme (milliseconds)	PAGO Scheme (milliseconds)	MOEO Scheme (milliseconds)	MOAV Scheme (milliseconds)	MOZO Scheme (milliseconds)	ACS Scheme (milliseconds)
1131	42187	52294	32994	120031	31703	113547	42826
2712	92843	83916	51203	83235	128125	148297	244524
4217	55000	127921	70793	390141	93312	224047	432543
6656	122609	172681	84256	161329	203125	286015	608651
9216	202640	218038	123750	906187	313484	391781	855701

Different types of files with different size are encrypted by seven numbers of text encryption schemes. The encryption time needed by the text encryption schemes are represented in Table 9.4 where execution time is calculated in milliseconds.

Figure 9.3 graphically represents encryption time for different files encrypted by the implemented text encryption schemes.

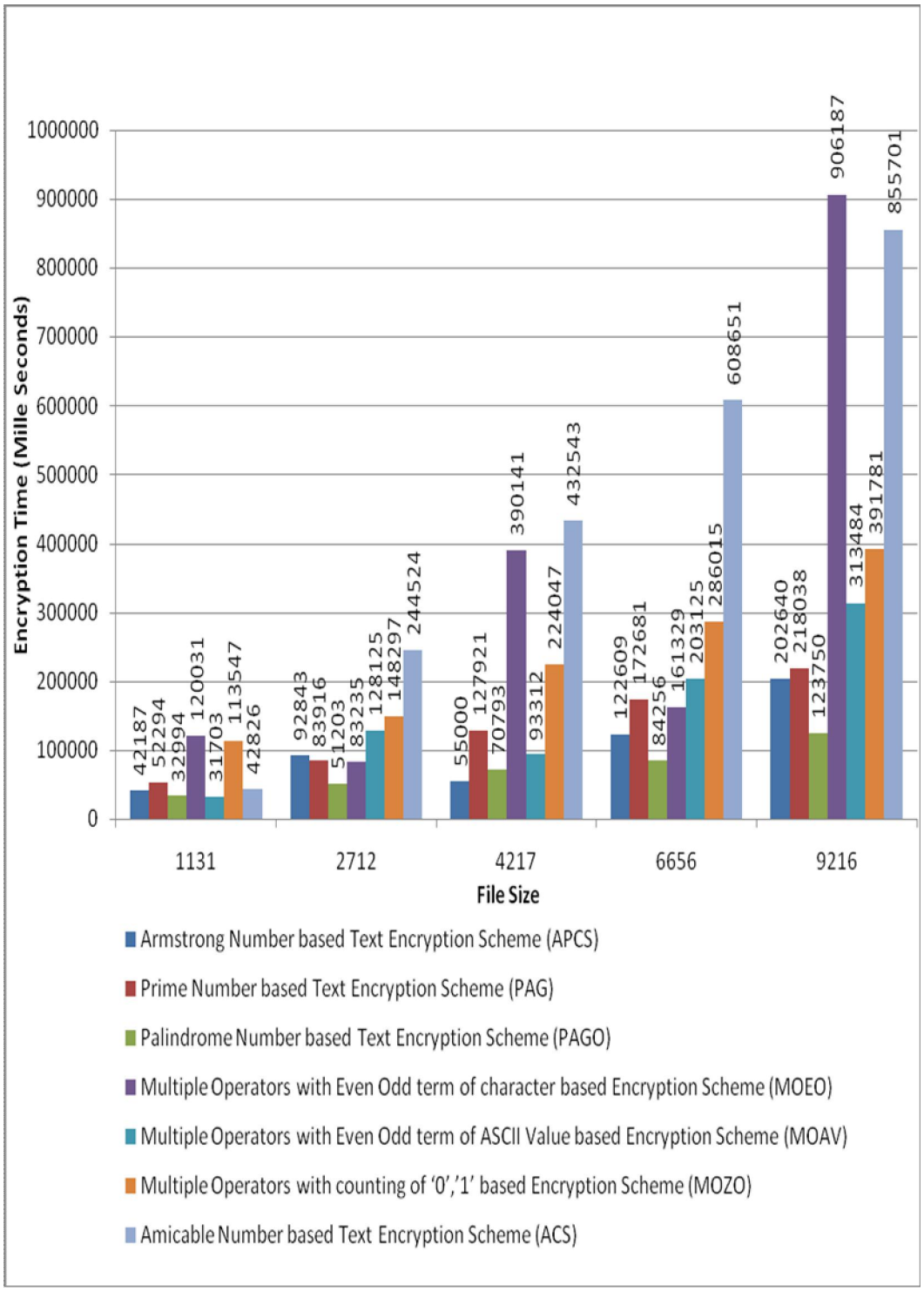

Figure 9.3: Representation of Encryption Time for Different Files by APCS, PAG, PAGO, MOEO, MOAV, MOZO and ACS Schemes

Table 9.5 and Figure 9.4 represent the Chi-Square values (calculated as per the equation 3.1 mentioned in the chapter 3) for different files which are encrypted by the implemented text encryption schemes where the performance of MOZO and APCS schemes are best compared to other schemes as the files encrypted by those schemes provide highest Chi-Square values compared to the encrypted files by other schemes.

Table 9.5: Chi-Square Values of Different Files encrypted by APCS, PAG, PAGO, MOEO, MOAV, MOZO and ACS Schemes

File size (Bytes)	APCS Scheme	PAG Scheme	PAGO Scheme	MOEO Scheme	MOAV Scheme	MOZO Scheme	ACS Scheme
1131	527132.03	26221.9707	51633.5039	8216.072266	68012.91406	14604.62891	1849.76
2712	1986680.8	317208.0313	48514.3555	2712	110543.2891	74822.42188	7212.23
4217	493531.47	23029.44531	1248575.63	70892.25	191009.5156	147652.125	10640.60
6656	6457562.5	2302158	874256.063	368832.0313	3065705.25	7593299	44474.78
9216	283393.25	1799318.375	168168.656	210041.2031	247490.7813	1782321.875	59162.72
10240	3366700.3	2177440	1364625.5	1753322.625	569319.3125	10600647	75107.37

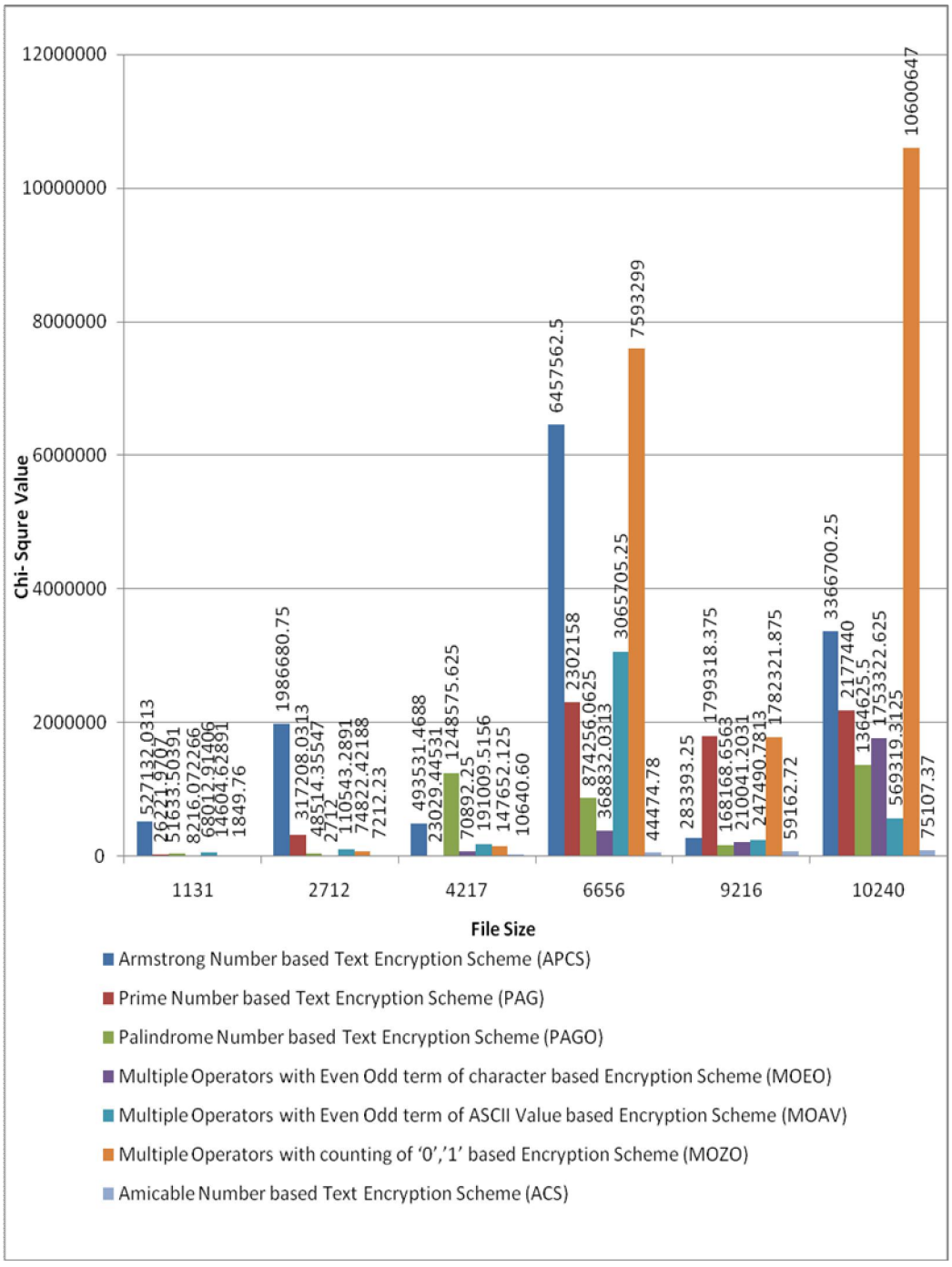

Figure 9.4: Graphical Representation of Chi-Square Values of Different Files encrypted by APCS, PAG, PAGO, MOEO, MOAV, MOZO and ACS Schemes

Table 9.6 and Figure 9.5 show Degree of Freedom values (calculated as per the equation 3.2 mentioned in the chapter 3) for multiple numbers of files which are encrypted by implemented text encryption schemes where APCS and ACS schemes are best performers compared to other schemes as the degree of freedom values are highest for most of files encrypted by APCS or ACS scheme.

Table 9.6: Degree of Freedom Values of Different Files encrypted by APCS, PAG, PAGO, MOEO, MOAV, MOZO and ACS Schemes

File size (Bytes)	APCS Scheme	PAG Scheme	PAGO Scheme	MOEO Scheme	MOAV Scheme	MOZO Scheme	ACS Scheme
1131	252	165	166	228	175	181	254
2712	254	202	202	190	212	211	255
4217	250	244	215	250	245	247	255
6656	249	229	229	241	234	234	255
9216	251	245	246	251	248	247	255
10240	254	253	254	248	247	248	255

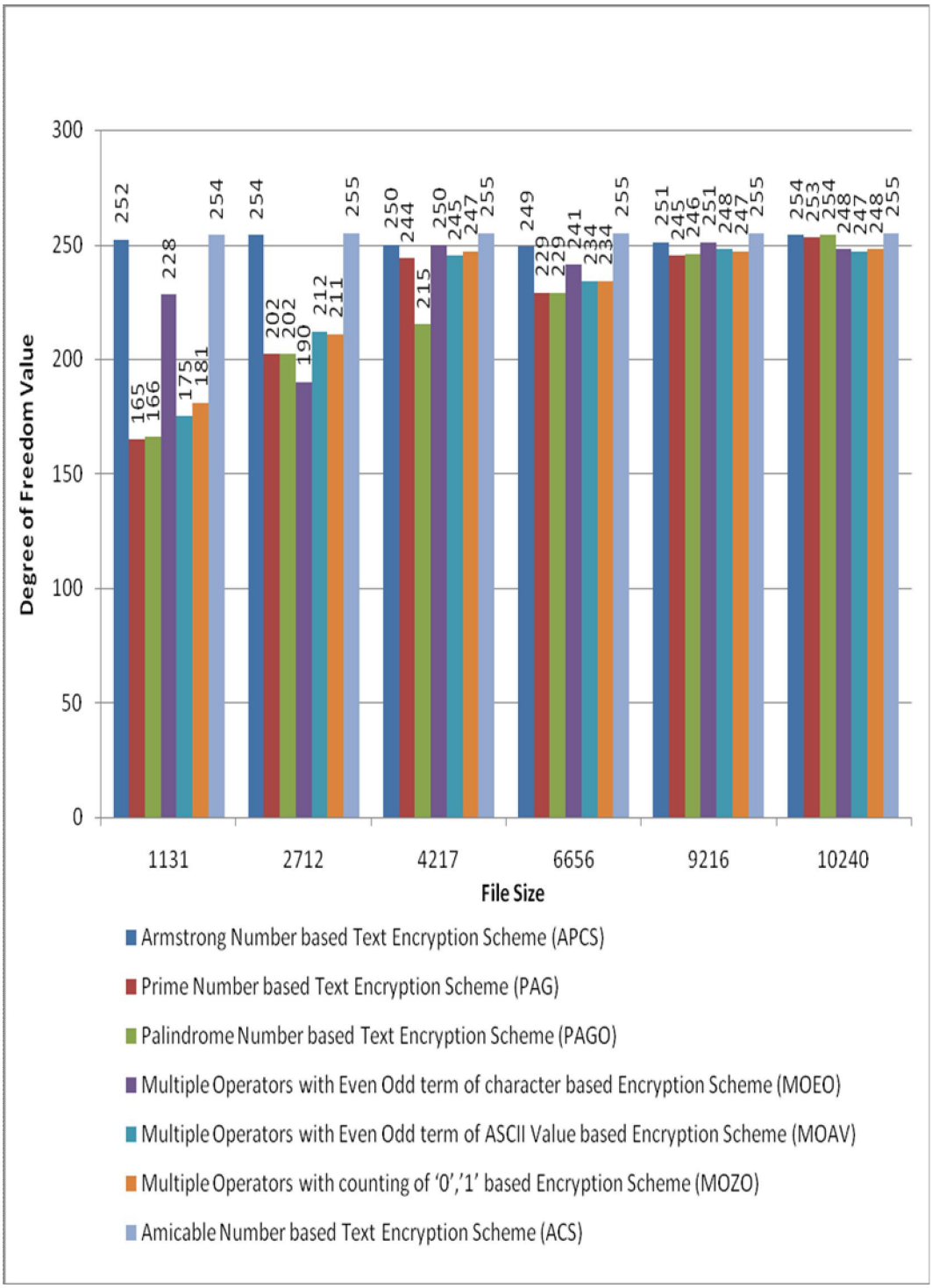

Figure 9.5: Graphical Representation of Degree of Freedom Values of Different Files encrypted by APCS, PAG, PAGO, MOEO, MOAV, MOZO and ACS Schemes

Table 9.7 shows the result of summarized performances assessment of implemented different text encryption schemes depending upon different parameters or criteria. An abbreviation of ê is applied here where average performance is represented by ' ê ', good performance is represented by ' ê ê ', very good performance is represented by ' ê ê ê ' and extremely good performance is represented by ' ê ê ê ê '. Counting of ' ê ' defines the performance assessment. From the summarized result it is clear that the APCS scheme is the best performer followed by PAG and MOZO schemes. PAGO and MOAV schemes jointly hold the third position. ACS and MOEO schemes are the worst performers among all the schemes.

Table 9.7: Result of Summarized Performance Assessment of APCS, PAG, PAGO, MOEO, MOAV, MOZO and ACS Schemes

Name of Text Encryption Scheme	**Name of Parameters / Criteria for Performance Assessment**		
	Encryption Time	**Chi-Square Value**	**Degree of Freedom Value**
APCS Scheme	ê ê ê ê	ê ê ê ê	ê ê ê ê
PAG Scheme	ê ê ê	ê ê ê	ê ê ê
PAGO Scheme	ê ê ê ê	ê ê	ê ê
MOEO Scheme	ê ê	ê ê	ê ê ê
MOAV Scheme	ê ê ê	ê ê	ê ê ê
MOZO Scheme	ê ê	ê ê ê ê	ê ê ê
ACS scheme	ê ê	ê	ê ê ê ê

C. Performance Analysis for Image Encryption Building Blocks

Implementation of even odd block based digital enveloping and cumulative image encryption based on image partitioning, key based encryption and digital enveloping have increased the security for image encryption. Applying of user defined pixels repositioning algorithm and user defined Bit Wise Masking for Alternate Sequence

(BWMAS) operation have imposed great security over existing image encryption schemes. Table 9.8 and Figure 9.6 represent the PSNR (Peak Signal-to-Noise Ratio) (calculated as per the equations 3.4 mentioned in chapter 3.) values for multiple files which are encrypted by implemented image encryption schemes where EODE scheme is best performer compared to CIDKP and CISP scheme as the PSNR values are highest for the files encrypted by EODE scheme.

Table 9.8: PSNR Values of Different Files encrypted by EODE, CIDKP and CISP Schemes

Image File Size (KB)	EODE Scheme	CIDKP Scheme	CISP Scheme
335	56.9883 dB	52.2793 dB	44.3506 dB
313	56.8563 dB	52.314 dB	44.9504 dB
114	56.6661 dB	52.3591 dB	44.9405 dB
189	56.4871 dB	52.4794 dB	45.1287 dB
287	57.4712 dB	53.5654 dB	44.5293 dB

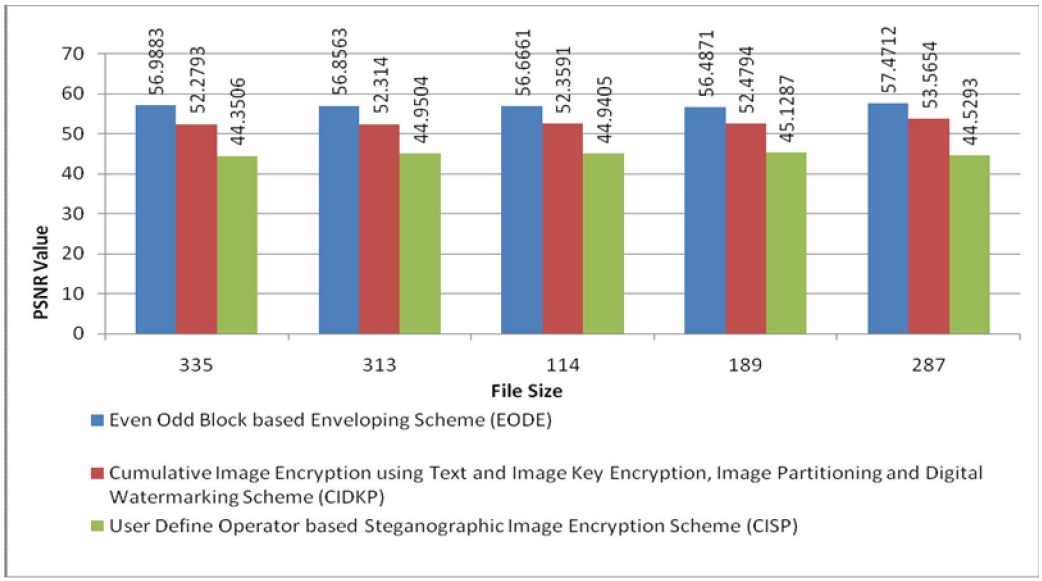

Figure 9.6: Graphical Representation of PSNR Values of Different Files encrypted by EODE, CIDKP and CISP Schemes

Table 9.9 and Figure 9.7 show SSIM (Structural Similarity Index) (calculated as per the equations 3.5 mentioned in chapter 3) values for different files encrypted by newly implemented image encryption schemes where performance of EODE scheme is best as the SSIM values for EODE scheme's encrypted files are closer to '1' compare to CIDKP and CISP scheme. Encrypted files of CIDKP schemes also provide good results.

Table 9.9: SSIM Values of encrypted Files using EODE, CIDKP and CISP Schemes

Image File Size (KB)	EODE Scheme	CIDKP Scheme	CISP Scheme
335	99.8445	99.7589	98.5057
313	99.8808	99.6737	98.5274
114	99.7278	99.7341	96.3594
189	99.8242	99.5728	97.7845
287	99.8888	99.7285	97.9717

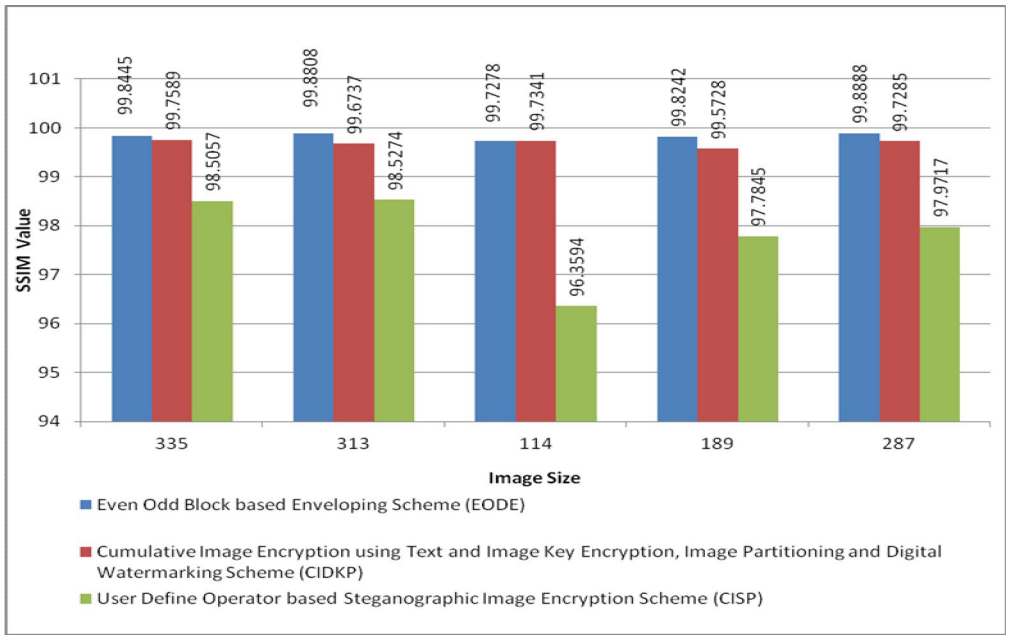

Figure 9.7: Graphical Representation of SSIM Values of encrypted Files using EODE, CIDKP and CISP Schemes

Table 9.10 and Figure 9.8 represent Universal Image Quality Index (Q-INDEX) values (calculated as per the equations 3.6 mentioned in chapter 3.) for files encrypted by developed image encryption schemes where EODE scheme is the best performer as Q-INDEX values of EODE scheme's encrypted files are more closer to '1' compare to CIDKP and CISP scheme.

Table 9.10: Q-INDEX Values of Files encrypted by EODE, CIDKP and CISP Schemes

Image File Size (KB)	EODE Scheme	CIDKP Scheme	CISP Scheme
335	0.9999880631622720	0.9999650713759340	0.9997367588816640
313	0.9999931169160950	0.9999816768805310	0.9999064003952400
114	0.9999593505533340	0.9999090380077020	0.9994570276889950
189	0.9999650494186980	0.9999344989697040	0.9996285877166560
287	0.9999869927464400	0.9999751197837930	0.9997965813942100

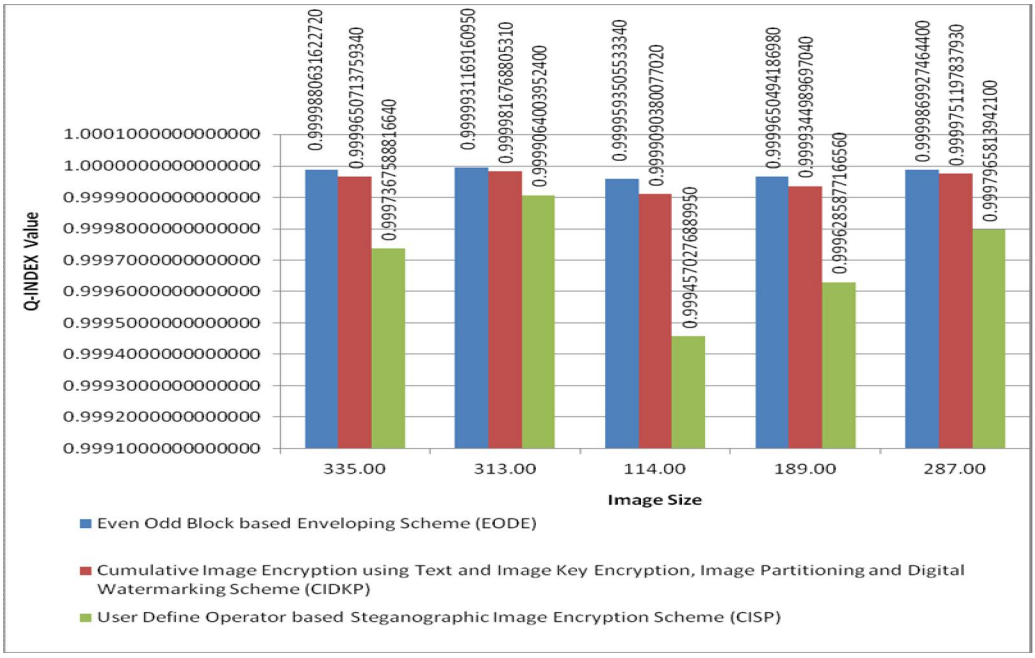

Figure 9.8: Representation of Q-INDEX Values of Encrypted Files using EODE, CIDKP and CISP Schemes

Table 9.11 and Figure 9.9 show Correlation Coefficient (calculated as per the equations 3.8 mentioned in chapter 3.) values for different files encrypted by designed image encryption techniques where CISP scheme's performance is best as Correlation Coefficient values of the files encrypted by CISP scheme are farthest from '1' compare to CIDKP and EODE scheme.

Table 9.11: Correlation Coefficient Values of Files encrypted by EODE, CIDKP, and CISP Schemes

Image File Size (KB)	EODE Scheme	CIDKP Scheme	CISP Scheme
335.00	1.0000	1.0000	0.9998
313.00	1.0000	1.0000	0.9999
114.00	1.0000	0.9999	0.9995
189.00	1.0000	0.9999	0.9997
287.00	1.0000	1.0000	0.9999

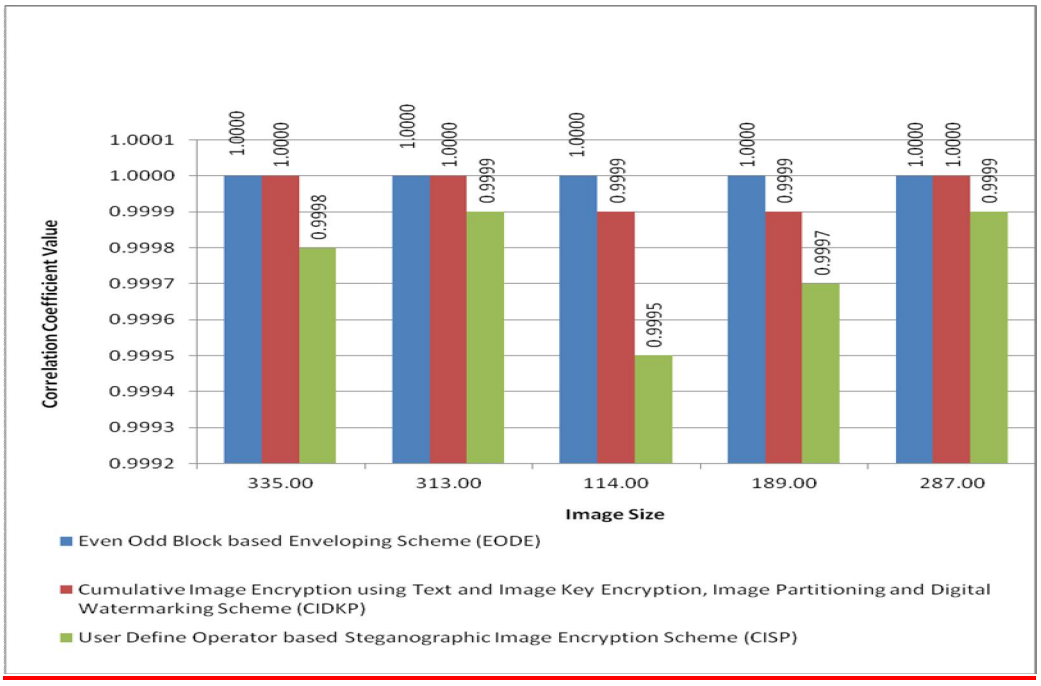

Figure 9.9: Representation of Correlation Coefficient Values of Encrypted Files using EODE, CIDKP and CISP Schemes

Table 9.12 and Figure 9.10 display the BER (Bit Error Rate) (calculated as per the equations 3.7 mentioned in chapter 3) values for several files encrypted by implemented image encryption methods where performance of EODE scheme is best as BER values for EODE scheme's encrypted files are extremely less compare to CIDKP and CISP scheme.

Table 9.12: BER Values of Encrypted Files using EODE, CIDKP and CISP Schemes

.

Image File Size (KB)	EODE Scheme	CIDKP Scheme	CISP Scheme
335.00	0.002603645833333330	0.007579340277777770	0.041733159722222200
313.00	0.002580815972222220	0.007537586805555550	0.041436545138888800
114.00	0.002566840277777770	0.007487326388888880	0.041270486111111100
189.00	0.002575086805555550	0.007481510416666660	0.034456163194444400
287.00	0.002038307604345340	0.005819788178278740	0.041753450951564100

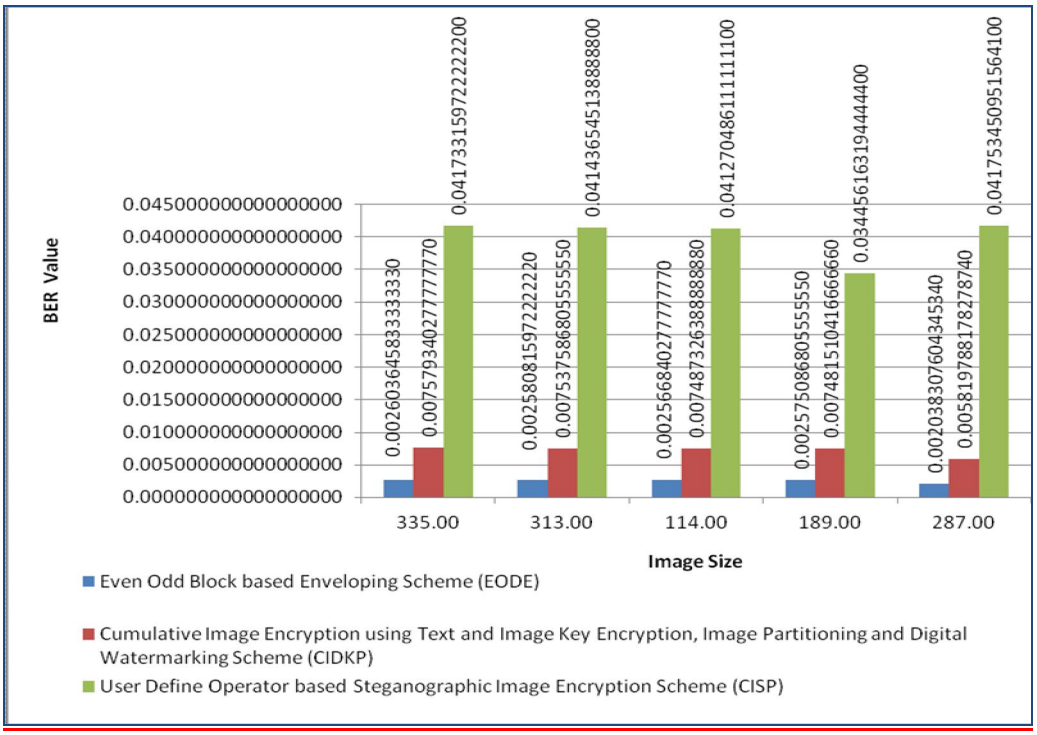

Figure 9.10: Representation of BER Values of Encrypted Files using EODE, CIDKP and CISP Schemes

Table 9.13 and Figure 9.11 represent the encryption time in milliseconds for different files encrypted by implemented image encryption techniques where performance of CIDKP scheme is best as the encryption time for encrypting files using CIDEK scheme is least compare to EODE and CISP scheme.

Table 9.13: Encryption Time for Different Files using EODE, CIDKP, and CISP Schemes

Image File Size (KB)	EODE Scheme (milliseconds)	CIDKP Scheme (milliseconds)	CISP Scheme (milliseconds)
335.00	32087	27153	39680
313.00	30780	31720	36046
114.00	18721	25747	33414
189.00	16620	24547	52468
287.00	49721	25447	41790

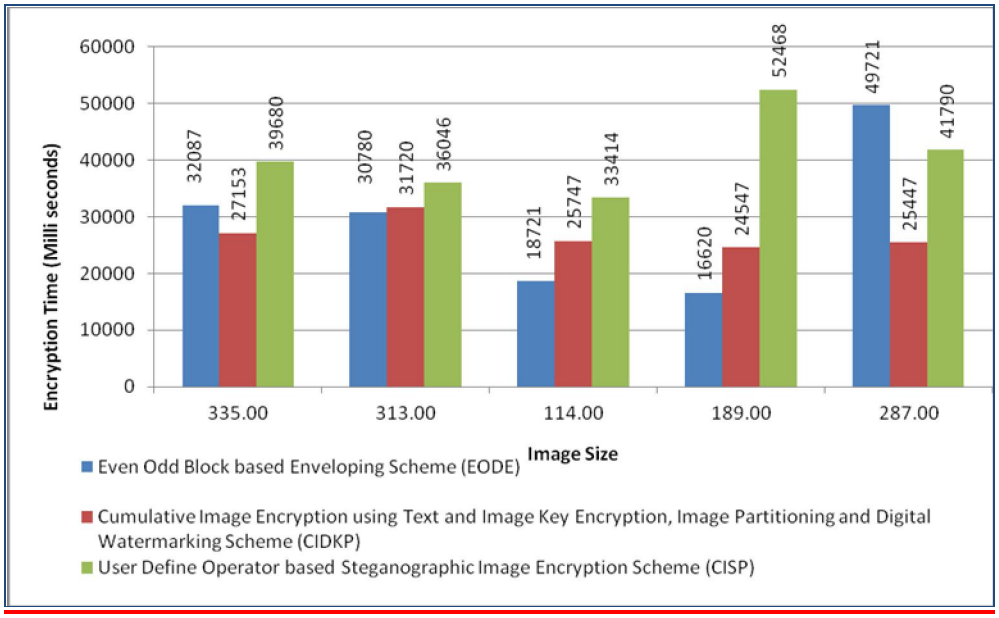

Figure 9.11: Representation of Encryption Time of Files encrypted using EODE, CIDKP and CISP Schemes

Table 9.14 displays summarized performances assessment results of implemented image encryption techniques depending upon different criteria or parameters. ‘ ê ’ is used as an abbreviation where average performance is abbreviated as ‘ ê ’, good performance is abbreviated as ‘ ê ê ’, very good performance is abbreviated as ‘ ê ê ê ’ and extremely good performance is abbreviated as ‘ ê ê ê ê ’. Performance assessment is defined by counting of ‘ ê ’. From the summarized performance table it is clearly shown that CIDKP scheme with multiple security layers is the best performer followed by EODE scheme holding second positions. CISP scheme has got third positions among all the schemes.

Table 9.14: Summarized Performance Assessment Results of EODE, CIDKP and CISP Schemes

Name of Parameters / Criteria for Performance Assessment	**Name of Image Encryption Scheme**		
	EODE Scheme	**CIDKP Scheme**	**CISP Scheme**
PSNR Value	ê ê ê ê	ê ê ê ê	ê ê ê
SSIM Value	ê ê ê ê	ê ê ê ê	ê ê ê
Q-INDEX Value	ê ê ê ê	ê ê ê ê	ê ê ê
Correlation Coefficient Value	ê ê	ê ê ê	ê ê ê ê
BER Value	ê ê ê ê	ê ê ê	ê ê
Encryption Time (Milliseconds)	ê ê ê	ê ê ê ê	ê ê
Numbers of security layers	ê ê	ê ê ê ê	ê ê ê

9.3. Summary of Research

Chapter 1 discusses a brief idea about encryption, decryption, cryptography, Special numbers, the structure of a color image, CAPTCHA(Completely Automated Public Turing Test), OTP(one time password), digital enveloping and steganography which are closely related with this thesis.

Chapter 2 deals with detailed literature surveys of CAPTCHA and OTP based user authentication, cryptography, private key based text encryption, image encryption and steganography. The main focus is to carry out detail background study on user authentication, text encryption and image encryption domain.

Chapter 3 of this thesis describes different stander parameters, attacks, algorithms and security tools to access the performances of newly developed building blocks (i.e. algorithms) and as well as the implemented security toolkit.

Chapter 4 deals with newly implemented CAPTCHA Code based on User Personal information and Likings (CCUPL) based scheme and the performance of the scheme is measured by analyzing the protection over standard attacks. An appreciable outcome is measured in respect of that comparison.

It also describes newly introduced Secret Value based on Randomize One Time Password scheme (SVROTP) and Numeric and biometric Image based One Time Password scheme (NIOTP). Similarly, performances of the schemes are measured in respect of protection over standard attacks.

Chapter 5 includes newly implemented Prime number with Alphabetic Group based text encryption Scheme (PAG) and Palindrome number with Alphabetic Group and Operator based text encryption Scheme (PAGO) where appreciable performances are accessed as compared to standard algorithms like AES, Twofish and Serpent.

It also contains newly introduced Amicable number with Cipher Sequencing based text encryption Scheme (ACS) and Armstrong and Perfect number with Cipher Sequencing based text encryption Scheme (APCS). Outputs of the schemes are compared with AES, Triple DES and Blowfish algorithm where a satisfactory result is provided by the implemented algorithms.

Chapter 6 describes newly introduced Multiple Operator and Even Odd position based text encryption (MOEO), Multiple Operator and ASCII Value based text encryption (MOAV) and Multiple Operator and number of Zeros and Ones based text encryption (MOZO) based text encryption schemes where a separate private key is generated and used for encrypting each of the plain text's character. Satisfactory performances are measured in respect of different standardized parameters like encryption and decryption time, Pearsonian chi-square value and degree of freedom value.

Chapter 7 includes newly implemented Even Odd block based Digital Enveloping scheme (EODE) and Cumulative Image encryption using Steganographic scheme with Pixel repositioning (CISP) where user defined pixels repositions procedure and Bitwise Masking and Alternate Sequence (BWMAS) operation are introduced for the first time. Both Schemes produce satisfactory results as compared with the standard parameters.

It also contains a new Cumulative Image encryption scheme using Digital enveloping, Key based encryption with image Partitioning (CIDKP) where an image is encrypted in multiple levels and produce appreciable outcomes with better security.

In chapter 8, brief structures of implemented security toolkit along with the detailed description of each of its building blocks are described. Newly implemented user defined methodologies which have been used for building blocks are discussed here.

Chapter 9 represents the analysis and comparisons between the newly implemented building blocks in respect of stander parameters. It includes the summary of entire research and the future scope of work.

9.4. Future Scope of Work

The security toolkit is implemented for a standalone system. An open access online version may be implemented in the future where an additional layer of security will be developed to restrict unauthenticated access from open communication channels through which end user will be interacting with the security toolkit.

User authentication based building blocks use biometric images and user likings for CAPTCHA or OTP generation which are taken as inputs. A large number of user likings and biometric images may be taken as inputs where randomly selected biometric images and user likings will be considered for OTP or CAPTCHA generation. This idea may be implemented in future which imposes additional security over the existing system.

Some algorithms used for text encryption building blocks which provide great security, but take large amount of times at the time of calculating N^{th} term (where N is a user defined long integer), if the N^{th} term is very much higher. Algorithms with new logic may be implemented for the same purposes in future which reduce execution time though the N^{th} term is very much higher.

Algorithms implemented for image encryption based building blocks provide satisfactory level of security as compared to standard algorithms but an additional level of memory is required for storing and transmitting image information between end users. A memory management algorithm may be implemented in future for sharing the same memory location dynamically between different images. Thus memory consumption will be reduced.

Implemented security toolkit provides security for user authentication, text and image data. Blocks for audio and video data will be implemented and incorporated with existing security toolkit in future.

Standard encryption algorithms for text, image, audio and video data will be implemented and incorporated with the existing security toolkit in future which will increase the acceptance of the security toolkit.