

University of Baghdad

College Name	College of Education for Women		
Department	Computer Science		
Full Name as written in Passport	Dr. Ayad A. Abdulsalam		
e-mail	ydsalam@yahoo.com		
Career	<input type="radio"/> Assistant Lecturer	<input checked="" type="radio"/> Lecturer	<input type="radio"/> Assistant Professor
	<input type="radio"/> Master	<input checked="" type="radio"/> PhD	
Thesis Title	Partial Encryption Using Clock-Controlled Random Generator of Wavelet Compressed Visual Data		
Year	2005		
Abstract	<p>Image and video applications such as the World Wide Web and video conferencing have increased dramatically in the recent years. When communication bandwidth or storage is limited, data is often compressed. On the other hand, encryption is also performed if it is necessary to protect the privacy of the users. A conventional solution consists of the systematic encryption of all data. When dealing with images, this approach is inconvenient because the data needs to be processed in its entirety before users can gain any insight. As well, the decryption task requires large amounts of processing power. This thesis shows how partial encryption can match applications requirements without the overhead of full encryption. Several schemes mixing encryption and image compression are discussed. Then, we focus on a technique that implements partial encryption of images. The technique is built to reduce the encryption time and keep the compliant with the wavelet format. An algorithm using clock controlled random generator is proposed to encrypt only selected part of the compressed data, selection based on exponential distribution plotted as Pie wheel is proposed. Partial encryption is applied to wavelet image compression algorithm in this thesis. Finally, a new scheme by exploiting a technique named Difference Matrix is proposed, the mean (d) of the absolute of the difference values, the energy (E), and entropy (n) values are calculated for using as measures to determine the rate of sufficient encryption, (sufficiency depends on the application) by using histogram of encrypted image without the need to compare with original one. The results of testing the proposed system are encouraging for the still images, resulting in a significant reduction in encryption and decryption time. The proposed partial encryption scheme is fast, secure, and does not reduce the performance of the underlying compression algorithm.</p>		