International Journal of Innovation in Computer Science and Information Technology
Vol.6, NO.1, P:1-17
Received: 08 May 2025
Accepted: 07 February 2026

Maintaining the privacy of users in sharing and adjusting interests in Instagram social networks

Ebrahim Atashkade
computer department, Ahvaz Branch, Islamic Azad University, Ahvaz, Iran.
Seyed Mohammad Safi
Assistant Professor of computer department, Islamic Azad University, Ahvaz, Iran.

Abstract

Along with the growth of mobile and online social networks, internet users can exchange information easily. In order to match, the user must reveal his/her personal interests and information to recognize common cases among them. In some cases, users don't like to reveal all of their interests and personal information to others. They only want to fully reveal their interests if they are sure that there is a common interest between them and the intended user. Maintaining the privacy is one of the basic needs of each person in everyday life, that's why it has become one of the most important concerns of people in the virtual world. The purpose of this study was Maintaining the privacy of users in sharing and adjusting interests in Instagram. This study is looking for suitable methods for sharing and adjusting interests in Instagram with high security and convenient availability of information for the user which is evaluated by MANTHK method and is compared with aggressive background knowledge. In comparison of this method with other methods on MicroFTV dataset, regardless of the level of user privacy, the proposed method preserves the structural features of the network, better. However, all of the methods provide privacy for nodes in one level. Afterwards at the end of the research the proposed method is compared with a method without personalization and we have displayed that if every user has Safety sharing based on the needs of privacy, then efficiency of data can be increased.

Keywords: privacy, sharing, adjusting the interests, Instagram social networks.

Introduction

Along with the growth of mobile and online social networks, internet users can exchange information easily; social medias of mobile (MSN) including new attitudes in mobile technology which has combined wireless connection with social media. One of the most famous usages and the advantages of mobile social networks is adjusting the profile. This ability helps the users to find their favorite users (1). For instance, in their social life in making friends and finding people with the same interests. Therefore, this useful method is used to identify common interests but some issues are considered (2).

In order to match, the user should reveal his/her interests and personal information with other users to identify common cases among them. In some cases, users would not like to reveal all of their interests and personal information with other users. If they are confident that there is a common interest between them and the intended user, they would like to reveal all of their interests and personal information (3).

Security and privacy are the necessary condition to develop mobile social networks at the age of major data, however, the scheme of security usually needs a complex and efficient implementation. One of the interesting differences between social networks of Instagram and web based social networks is that the usage in (MSN) is identified based on a set of serial numbers (4).

While web based social networks they are identified by ideal fields and its clear example is phone number in mobile networks and license number in vehicle networks. We develop a lightweight public key application encoding scheme by taking the advantage of this slight difference and display the application for mobile networks, we have called these schemes encoding based on serial number (SNBE). Our scheme is based on a proven security in an assumed standard model (DBDH), while encoding text includes of three elements (5).

encoding based on serial number (SNBE) in those systems IDs are classified by serial numbers. In our system, the encoder labels every encoding text by a serial number. Every personal key is also connected by a serial number that determines which encoding key can decode. Each part is allowed to make a public key

Received: 08 May 2025
Accepted: 07 February 2026

from an identified serial number therefore, everyone can encode messages with no key pre-distribution between individual components (6).

The purpose of this study is to improve adjusting protocols and helping Instagram users. In order to safe adjusting without revealing Instagram and adjusting personal information is unnecessary. Helping this study in social networks, Instagram is as followings: a secure and protective privacy mechanism is presented to identify common interests in order to protect privacy and security of the user among attacks, which along with it a user is limited to one mobile. Implementing protocol and comparing it with existed methods, has determined that this protocol can protect from the user against several attacks without any destruction performance. We present a safety and privacy mechanism to identify common interests among users. Unlike the existing methods, the non-disclosure of user interests and confidential information to a trusted third party reduced absolute presumption of reliability in the third party. Questions of the study include: 1- Is it possible to upgrade privacy by feature-based encoding according to specific features of the Instagram social network? 2- Is it possible to protect privacy by feature-based encoding of Instagram social network through sharing?

Proposed method

Related approaches to graph:

A) Exploring of subgraphs: exploring of subgraphs is one of the tasks of link mining which explores similar subgraphs in couples of graphs. The purpose is finding a set of graphs which are similar to main graphs.

B) Classifying the graph: the purpose of classifying the graph is classification of the whole graph based on a special category. Independent classification of each node in a large graph is boring and sometimes is impractical, and maybe useful and available information of other nodes will be ignored.

In this section a modern method is presented to achieve *(h.g)* safety degree to protect privacy of users in sharing and adjusting interests of social network which is called MANTHK, in order to secure data which became a haven for maintaining privacy information, secure and confident protection and also make a connection between personal information, which along appropriate duration, data will differ for values, so that there is a good connection between storage, maintaining personal information and reduction of information loss. MANTHK algorithm for information, has produced equivalent data and then performs privacy process for sharing equivalent data. And $h.g$ will be achieved. MANTHK include three main steps: personalized separation, Secure protection of degree sequences and graph reconstruction. First of all, personalized micro aggregation algorithm is applied which is called MicroFTV on a G social graph which optimally separates a set of V(G) nodes in C_G series including $-\omega$.

In this study, while maintaining the privacy of the edge, structural destruction has decreased rather than other methods, and privacy of sensitive nodes will be considered more. In the proposed method, edge of sensitive nodes may change and increase and changes of edges in these nodes are given priority.

Relatively more efforts will be done in grouping and labeling each node in the graph.

C) Generative models based on graph: Generative model for graphs try to comprehend features of the network. According to network input, generator models can generate a new network which is similar to input. They can use the model correctly with similar construction and data distribution.

($-\omega$ cluster) by assuming social graph of G, $-\omega$ is the cluster of subsets, $C \subseteq V\ (G)$ which the number of existed nodes is

Received: 08 May 2025
Accepted: 07 February 2026

between ω_{max} and $2\omega_{min}$-1. ω_{max} and ω_{min} weight of node with the highest privacy level and wight of node with the lowest privacy level in C respectively. Formally,

$$\omega_{max} \leq |C| \leq 2\omega_{min} - 1\,. \qquad (1)$$

while

$$\omega_{max} = \max_{v_i \in C} \omega\big(\theta(v_i)\big). \qquad (2)$$

$$\omega_{min} = \min_{v_i \in C} \omega\big(\theta(v_i)\big). \qquad (3)$$

Then degree sequence of $d_{\tilde{G}}$ will be generated by using an optimal algorithm based on particle swarm which is called Particle FTV. Input of this algorithm is C_G and the output of that degree sequence is close to the optimal *(h. g)* secured degree in $d_{\tilde{G}}$ sharing. For this purpose, some of the existed nodes in $-\omega$ cluster changes to $C_{i.j} \in e_G$ to equal all of the degrees of existed nodes in $C_{i.j}$ and Δ*1* and Δ*2* will be minimized in relations of 4 and 5.

$$\Delta_1 = \textstyle\sum_{i=1}^{n} |d_G(v_i) - d_{\tilde{G}}(v_i)|. \qquad (4)$$

$$\Delta_2 = \textstyle\sum_{i=1}^{n} |d_G(v_i) - \sum_{i=1}^{n} d_{\tilde{G}}(v_i)|. \qquad (5)$$

Finally, by using a manipulation edges of graph algorithm which is called MicroFTV, $\tilde{G}$ graph will be made. $\tilde{G}$ is a social graph of (*h. g)* secured degree in sharing, which is made due to the $d_{\tilde{G}}$ degree sequence. Three main steps of MicroFTV are presented in figure 1.

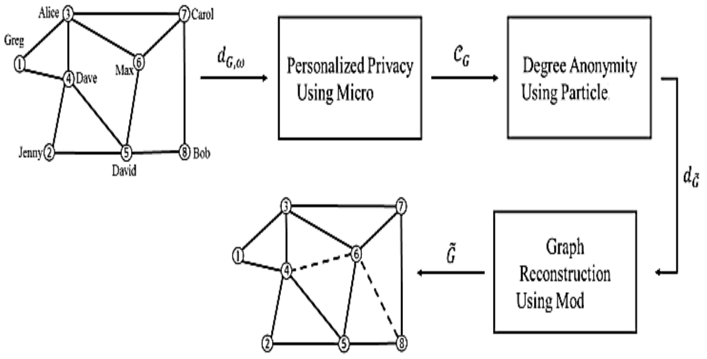

Alice
Carol
Greg
Dave
Max
Jenny
David
Bob
1
2
3
4
5
6
7
8
$d_{G,\omega}$
Personalized Privacy Using Micro
C_G
Degree Anonymity Using Particle
$d_{\tilde{G}}$
Graph Reconstruction Using Mod
$\tilde{G}$

Figure 1: Three main steps of MicroFTV

The personalized degree sequence of *Φ*

$$(\phi_G = \langle \phi_1 . \ \ldots . \phi_n \rangle \qquad (6)$$

While $\varphi_i = (d_i . \omega_i)$ is a degree-weight pair. $d_i = d_G(v_i)$ equals to node degree of $v_i$and $\omega_i = \omega(\theta(v_i))$ equals to the weight of v_i node.

For more simplicity, we assume that pair of existed degree-weights in Φ_G are arranged based in order of weight and then in descending order of degree. More precisely, for all of the *i*<*j* it has happened in $\omega_i > \omega_j$ یا$\omega_i = \omega_j$ and $d_i \geq d_j$. Then an oriented and weighted G_Φ are made from the main graph of G. a series of $V(G_\Phi) =$

Received: 08 May 2025
Accepted: 07 February 2026

$\{\varphi_i|\varphi_i\epsilon\Phi_G\}$ nodes equal to $\{\varphi_0\}$ which $\varphi_0 = (0.\delta)$ is a fake couple and is used as source node for G_Φ. For *i<j* in both groups of $\varphi_i.\varphi_j\epsilon V(G_\Phi)$ if it is $(\varphi_i.\varphi_j)\epsilon E(G_\Phi)$ and only if the relation 3-6 is established.

$$i + \omega_{i+1} \leq j \leq i + 2\omega_j - 1 \qquad (7)$$

In fact $\varphi_i.\varphi_j$ is corresponding with $-\omega$ cluster $C_{i.j} = \{v_{i+1}.\dots.v_j\}$. weight of edge $\varphi_i.\varphi_j$ is presented with $w_{i.j}$ and will be calculated by 8-3 relation.

$$w_{i.j} = \sum_{l=i+1}^{j}(d_l - \bar{d}_{i.j})^2. \qquad (8)$$

So that, $\bar{d}_{i.j}$ average of node degrees is in the $C_{i.j}$:

$$\bar{d}_{i.j} = \frac{1}{j-i}\sum_{l=i+1}^{j} d_l \qquad (9)$$

In the following, in order to find the shortest route $\eta(\varphi_0.\varphi_n)$ in G_Φ between φ_0 and φ_n nodes the algorithm of the shortest route is used. $-\omega$ existed clusters corresponding with existed edges in this route (7) will be added to ℓ_G.

In the following for calculating ℓ_G we apply the shortest route algorithm $\eta(\varphi_0.\varphi_8)$ on G_Φ graph. In figure 2 the only route between φ_0 and φ_8 a route includes these edges $E(G_\Phi) = \{(0.5).(5.8)\}$.

Therefore, optimal separation of sequence degrees is personalized which in this example equals to:

$$\mathcal{C}_G = C_{0.5} \cup C_{5.8} = \{\{1.2.3.4.5\}.\{6.7.8\}\} \qquad (10)$$

10-3 relation expresses that $\{1.2.3.4.5\}$ and $\{6.7.8\}$ nodes should be anonymous with each other and get the same amount of anonymity. As it is shown in the separation there is no node in the $G_\Phi$directional graph cluster without any rounds.

Proof. if searching of depth level on the graph does not generate any back edge, the directed graph has no round (8). According to the presented algorithm in figure 2, $(\varphi_i.\varphi_j) \in E(G_\Phi)$ is back age, if relation 6 is established and the prior arrangement is based on *i<j.*

Assume that directed edge is $(\varphi_i.\varphi_j) \in E(G_\Phi)$ and the first search of depth, products $(\varphi_i.\varphi_j)$ edge. Therefore, according to the algorithm, it is *j<i* which is a contradiction. Thus, if the result of the first search is the depth of directed graph $G_\Phi$includes no back edge, the graph has no round. Computational complexity of MicroFTV for $k^2 < logn$ equals to *o(nlogn).*

-by assuming social graph of g, MicroFTV node series of V(G), separates to the $-\omega$ optimal clusters of $\mathcal{C}_G$. To do this, first of all Φ_G personalized sequence degree is producing then arrangement algorithm applies with temporal complexity of *o(n log n)* on sequence degree which $n = |V(G)|$ equals to the number of existed members in V(G) series. In the following of the algorithm, directed and weighted graph of G_Φ is producing. G_Φ includes n+1 which the degree in each node is a maximum of k. finally the algorithm of the shortest route applies on the G_Φ to calculate n+1. Graph 3 of G_Φ is directed and without any round which the calculation of the shortest route in this graph with temporal complexity of *o (kn)* is applicable (9) therefore temporal complexity of MicroFTV is limited to $(\max(n \log n . k^2 n))$. For $k^2 < \log n$ temporal complexity equals to *o(n log n)*.

So that, $v_{r.s}(t)$ of update for each $-\omega$ cluster is $C_s \epsilon \mathcal{C}_G$ which is $s = 1. \dots . |\mathcal{C}_G|$ and *C₁* and *C₂* are acceleration constant. $r_{1.s}(t), r_{2.s}(t)$ and $r_{3.s}(t)$ are three random amounts in *{1.0}* range. Also, sigmoid function of $sig(v_{r.s}(t))$ is $v_{r.s}(t)$ for computation and is calculated from the following relation:

In the following y_r *(t)* is the best private condition and is calculated from the following relation:

$$y_r(t) = \begin{cases} y_1(t-1) & if \quad f(y_r(t-1)) \le f(x_r(t)). \\ x_r(t) & otherwise\,. \end{cases} \qquad (13)$$

Which *f*(0) is fit function and should be minimized.

After this step and in every repeat of *t*, $\tilde{y}(t)$ is updating as the best public condition:

$$\tilde{y}(t) = \underset{y_r(t) \,\in\, Y(t)}{argmin} f(y_t(t)) \qquad (14)$$

In this relation *y(t)* is a series of the best private conditions, all of the particles are in *S(t):*

$$Y(t) = \{y_r(t) | r \in S\} \qquad (15)$$

In fact, $\tilde{y}(t)$ chooses the best condition among the best conditions of particles. Finally, according to $\tilde{y}(t)$ the secured sequence degree $d^*_{\tilde{G}}$ is producing. To do this, for each $v_i \in V(G)$ node, $-\omega$ cluster, $C_s \in \mathcal{C}_G$ which include this node, is chosen. If there is $\tilde{y}_s(t) = 0$, the amount of $d^*_{\tilde{G}}(v_i)$ equals to $\lfloor \mu(C_s) \rfloor$, otherwise $d^*_{\tilde{G}}(v_i)$ equals to $\lceil \mu(C_s) \rceil$.

Computational complexity. Computational complexity of particleFTV algorithm equals to multiplying the number of summonses by two fitting functions in relation 14 and relation 15 in chronological order of calculating of these two functions. If the number of populations equal to *S* and repetitive number of the main ring would be *t* times, the number of summonses of fitting functions would be *ST* times. Execution time of each of the fitting functions need *O(n)*. therefore, Computational complexity of ParticleFTV algorithm equals to $0(St(2n))$.

3-3 particle representation

One of the important issues in design of FTV algorithm, is presenting potential answers as particles. To do this, we define every particle of $r \in S$ as a binary vector, as followings:

$$X_r = (X_{r.1} . X_{r.2} . \dots . X_{r.m}) \qquad (16)$$

this relation $m = |\mathcal{C}_G|$ equals to the number of $-\omega$ clusters in $\mathcal{C}_G$. In addition, each element of $X_{r.s} \in X_r$ is matching with $-\omega$ cluster of $C_s \in \mathcal{C}_G$ and for amount calculation $\Omega_r(C_s)$ in relation 17 will be used. $\Omega_r(C_s)$ determines anonymity of amount for all of the existed elements in C_s:

$$\Omega_r(C_s) = \begin{cases} \lfloor \mu(C_s) \rfloor & x_{r.s} = 0 \\ \lceil \mu(C_s) \rceil & otherwise \end{cases} \qquad (17)$$

International Journal of Innovation in Computer Science and Information Technology
Vol.6, NO.1, P:1-17
Received: 08 May 2025
Accepted: 07 February 2026

In relation 17, $\lfloor . \rfloor$and $\lceil . \rceil$ are lower round and higher bound respectively. In fact, each x_r is a $(h.g)$ secured degree in sharing and represents $d_{\tilde{G}}^{r}$. The average of degrees of all of the existed nodes in C_s is a wrong number. Formally:

$$\lfloor \mu(C_s) \rfloor \neq \lceil \mu(C_s) \rceil and |(C_s)| \notin \mathbb{Z} \tag{18}$$

Then in order to perform the reconstruction operation, amount of $x_{r.s}$ corresponding with each incorrect condition of x_r would be vice versa. In other words, if the amount of $x_{r.s}$ equals to zero we change its amount to 1 and vice versa. By doing this, we change odd values to even values in $d_{\tilde{G}}^{r}$ a sequence is – (0.1) which is presented by X_r particle.

In this study, two fitting functions evaluate the condition of each particle which are called f_1 and f_2 . assume the condition of particle X, function $f_1(X_r)$ and $f_2(X_r)$ respectively equal to sum and absolute sum, subtractions between degrees of each member V(G) node and its secured value which is produced according to X_r particle:

Fitting function

$$f_{۱}(x_r) = \left| \sum_{C_s \in \mathcal{C}_G} \sum_{v_i \in C_s} (d_G(v_i) - \Omega_r(C_s)) \right| \tag{19}$$

$$f_{۲}(x_r) = \left| \sum_{C_s \in \mathcal{C}_G} \sum_{v_i \in C_s} (d_G(v_i) - \Omega_r(C_s)) \right| \tag{20}$$

Final fitting function for particle is (X_r), weighted averages are f_1 and f_2 and is calculating with the following relation: (in this relation the value is $\alpha\epsilon[0.1]$ and is used by the user)

$$f(x_r) = \alpha . f_{۱}(x_r) + (1-\alpha) . f_{۲}(x_r) \tag{21}$$

Generally, in this study three main actions are used to manipulate the graph, which including movement of the edge, omitting the edge and adding the edge.

movement of the edge: despite the three edges of $v_{10}v_{20}v_3\epsilon V(G)$, if there are $(v_{10}v_3)\epsilon E(G)$ and $(v_{20}\ v_3) \notin E(G)$, therefore we omit $(v_{10}\ v_3)$ from E(G) and add the new edge of $(v_{10}\ v_3)$. This action is called movement of the edge. This action reduces the degree of v_1 one unit, and increases the degree of v_2 one unit and to be in a stable it would be 7_3. If we manipulate the social graph of G only with one movement action, then there is:

$$\sum_{i=1}^{n} d_G(v_i) = \sum_{i=1}^{n} d_{\tilde{G}}(v_i) \tag{22}$$

Omitting edge: Despite four nodes of $v_{10}v_{20}v_3\epsilon V(G)$, if there are $(v_{10}v_3).(v_{20}v_4)\epsilon E(G)$ and $(v_{30}v_4) \notin E(G)$, then we omit $(v_{10}v_3)$and $(v_{20}v_4)$ from E(G) and add $(v_{30}v_4)$ to it. This action is called omitting the edge. It reduces the degree of v_1 and $v_2$one unit and the stability degree would be v_1 and v_2. If we manipulate the social graph of G just by omitting the edge, there is:

$$\sum_{i=1}^{n} d_G(v_i) = \sum_{i=1}^{n} d_{\tilde{G}}(v_i) + 2 \tag{23}$$

Adding edge: despite two nodes $v_{۱}.v_{۲}\epsilon V(G)$ formula, if there is $(v_{10}v_2) \notin E(G)$ then we add $(v_1\ v_2)$ to the E(G). this action is called movement of the edge. It increases the degree of v_1 and $v_2$one unit.

Received: 08 May 2025
Accepted: 07 February 2026

If the social graph of G is manipulated just by adding, then there is:

$$\sum_{i=1}^{n} d_G(v_i) = \sum_{i=1}^{n} d_{\tilde{G}}(v_i) - 2 \tag{24}$$

Figure 2 represents three manipulating graphs

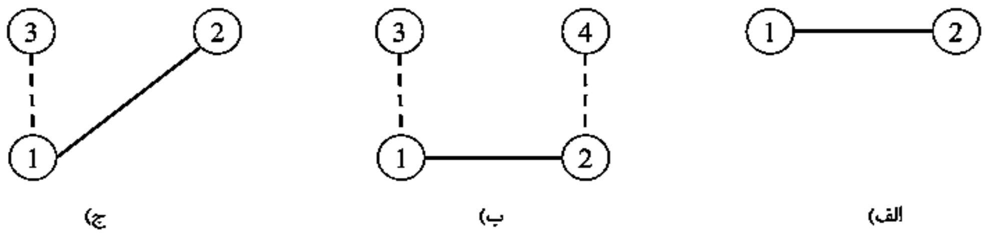


Figure 2- three manipulating graphs, A) adding edge, B) omitting edge, C) movement the edge. C)movement the edge. Dotted lines represent omitted edge and continuous lines are added edges to graph (10)

Manipulation of the graph starts by achieving a sequence of changes between dG and $d^*_{\tilde{G}}$ sequence degrees:

$$\sigma = d_G - d^*_{\tilde{G}} \tag{25}$$

σ is made by sequences of two series which σ^+ include nodes and their degree should be increased and σ^- include nodes which their degree should decrease. Also $\varsigma(d)$ expresses the sum of the elements in the sequence of degree d. formally

$$\begin{array}{l} \sigma^+ = \{v_i | \sigma_i > 0\} \\ \sigma^- = \{v_i | \sigma_i < 0\} \end{array} \tag{26}$$

$$\varsigma(d_G) = \sum_{i=1}^{n} d(v_i) \tag{27}$$

If the value of σ is a positive number, the sum of the total degrees in the main sequence degree is more secured than sequence degree. In this condition, first of all $\frac{\varsigma(d_G)-\varsigma(d^*_{\tilde{G}})}{2}$ omitting the edge on the graph would be done and then edge movement is done on the main graph to produce a secured graph.

If the value of σ is a negative number, the sum of the total degrees in the main sequence degree is less secured than sequence degree. In this condition, first of all $\frac{\varsigma(d^*_{\tilde{G}})-\varsigma(d_G)}{2}$ adding the edge on the graph would be done and then edge movement is done on the main graph to produce a secured graph.

According to the fitting function in (27) relation, the presented algorithm tries to set the value of the formula close to zero. Therefore, movement of the edge is done in this step the most. So that for each $v_i \epsilon \sigma^+$ and $v_j \epsilon \sigma^-$ node, one vk is selected to $(v_j . v_k) \epsilon E$. then $(v_j . v_k)$ edge, is omitted from the graph and $(v_j . v_k)$edge will be added to the graph. Then the degree node vi of one of them would be high, the degree node vi of one of them would be low, and the degree of vk of would be stable.

Movement set: despite the σ^+ and σ^- of a movement set include a bilinear mapping of a σ^+ on the σ^-.

International Journal of Innovation in Computer Science and Information Technology
Vol.6, NO.1, P:1-17
Received: 08 May 2025
Accepted: 07 February 2026

In other words, mapping happens in a sequence movement of each $v_j \epsilon \sigma^+$ to a $v_i \epsilon \sigma^-$ and include one or more $(v_i . v_j)$ pairs.

Mod FTV algorithm, develops the algorithm of particle swarm optimization [11] to create a displacement sequence. The main idea of this algorithm is fixed on the set of $\sigma^-$and a permutation produces from a set of σ^+ to minimize $f_3$in relation (28-3).

In this algorithm first of all population of S is quantifying and algorithm step is performing to meet the final condition.

The permitted number of fits summons in each repetion t> 0 is updated by the value of velocity t(v_r) and position t(x_r) for each particle:

$$v_r(t) = \omega v_r(t-1) \oplus c_1 r_1(t)(y_r(t-1) - x_r(t-1) \oplus c_2 r_2(t) (\tilde{y}_s(t-1) - x_r(t-1)) \tag{28}$$

$$x_r(t) = x_r(t-1) + v_r(t) \tag{29}$$

As it is noted, v_3 is a set of trenches. In calculating the value of v_3, the sum of condition and speed and subtraction there are two particle condition which we calculate them in the followings:

Subtraction of two conditions: assume that there are two conditions of x_i and x_j the subtraction between these two conditions can be expressed in a set of trenches. Therefore, the subtraction between these two conditions is in speed type.

Sum of condition and speed: by assuming existence of x_r particles and v_r speed, the $v_r + x_i$ result equals to a new condition of x_i'. For instance if there is x_r={1.2.3.4} and $v_r = \{(1.2).(2.3)\}$ then the new condition equals to {3,1,2,4} =x_i'.

In the following the value of y_r(t) is the best private condition which is calculated from this relation:

$$y_r(t) = \begin{cases} y_r(t-1) if\ f(y_r(t-1) \leq f(x_r(t)). \\ x_r(t) \quad\quad otherwise. \end{cases} \tag{30}$$

Which the fitting function is f(0) should be minimized.

After this step and each repetition of t, the best public condition of $\tilde{y}(t)$ is updating and $\tilde{y}(t)$ and Y(t) values are obtaining with relation 10 and relation 11 respectively.

Finally, according to $\tilde{y}(t)$ a set of movements are producing. So that, firstly σ^+ set is arranged base on the existed values in $\tilde{y}(t)$. Then for each $v_i \epsilon \sigma^-$ node and in each $v_i \epsilon \sigma^-$ node a pair of (v_i,u_i) is adding to a set of movement.

Computational complexity. Computational complexity of ModFTV algorithm equals to multiply of the number of summonses of the fitting function in relation (13) in each performance of this function. If the number of populations is equal to S and the number of repetitions of the main ring is t times, the number of summonses of the fitting function is St times. Run time once the fitting function into time need o(n(n+m)). therefore, computational complexity of ParticleFTV algorithm equals to O(St(n(n+m))).

Particle representation

As it is mentioned, one of the most important issues in designing an FTV algorithm is providing potential answers as particles. So that, we define each $r \epsilon S$ particle as a discrete vector as in the following:

Received: 08 May 2025
Accepted: 07 February 2026

$$x_r = (X_{r.1}.X_{r.2}.\dots.X_{r.m}) \quad (31)$$

In this relation there is $m = |\sigma^+|$ which is equal to the number of nodes in a set of σ^+. In addition, each element of $x_{r.s}\epsilon x_r$ is matching with index of a $v_i\epsilon\sigma^+$ node. In other words, a x_r permutation produces a set of σ^+.

Fitting function

In this study, to evaluate the position of each particle, we use a fitting function called f_3 (12). Assume that the particle condition is x_r, the function equals to $f_3\,(x_r)$ is equal to the difference of the sum of the shortest routes between each node in the main graph and the graph created after the edges are displaced by the permutation created by x_r. If we call the sum of the shortest route between two existed node in G graph η_G and we call the shortest route between two nodes v_i and v_i in the secured $\tilde{G}$ graph $\eta(v_i, v_j)$, $f_3\,(x_r)$ will be calculated fron relation 32:

$$f_3(x_r) = \left|\left(\sum_{i=1}^{n}\sum_{j=1}^{n}\eta(v_i.v_j)\right) - \eta_G\right| \quad (32\text{-}3)$$

Implementation of the proposed method

Evaluation model

In this chapter MANTHK method are evaluated for different values of *(h.g)*. The evaluations were performed by a machine with an Intel quad-corei7-2600 processor and 16 GB of main memory. The MANTHK method was evaluated on several datasets. Then, this method was evaluated and compared with other methods of social network sharing, regardless of the level of privacy and considering the level of privacy.

The data set features used in this evaluation are listed in table (1). These features include the number of nodes, the number of edges, the average degrees in the network, and the amount of sharing. The Polbook Database is a network of US political books which were sold by the Amazon Online Store. The dataset is housed in the UCI Network Database and was released in 2008 after the presidential election. The Maido dataset is a network of interconnected systems via the Internet in the Maido project, compiled in 2007. Amazon Database is a network of products which is offered by Amazon to buyers.

Table 1: The main data set used in research evaluation

network	node	edge	Average of degree	Amount of K
Polbook	1785	3265225	19.523	1
Maido	2635	16895	11.689	1
Amazon	35695	45692	2.378	1

Evaluation criteria

In order to compare the proposed algorithm and the presented algorithms for social network sharing, several criteria used in [14,15,13] were used to compare the structural features between the main social network and sharing in this thesis. These criteria include:

Density. The ratio of all of the existed edges to all of the possible edges in the graph is called density. This criterion is calculated by relation (2).

Transitive. Transitive is a kind of coefficient sharing. These criteria ase used to evaluate local rings close to node. This criterion is used to calculate the percentage of routes with the length of two which are those triangles obtained from relation (5).

The most special value in the neighboring matrix. Special value of A matrix, include some information about the existed rounds in the network.

Harmonic average at the smallest distance. This criterion was used for evaluating connection in social network graph and is as the same as the average distance or the average length of the route. Also, unlike of the average harmonized shortest distance was known as the comprehensive efficiency and was calculated from relation 33.

$$\frac{1}{h} = \frac{1}{n(n-1)}\sum_{i.j=1}^{n}\frac{1}{d(v_i.v_j)} \qquad (33)$$

in this relation $d(v_i.v_j)$ is the shortest route from vi to vj and n is the number of social network nodes.

As the same as the proposed method by Jang et. Al (16) the candidate set of h_1 is used to analyze database and table (2) is presented. In this method, firstly for each $v_i \in G$ node, h_1 is calculated. Then set of h_1 candidate is calculating in relation 34.

$$cand_{H_1} = \{V_j \in V \uparrow h_1(V_i) = h_1(V_j)\} \qquad (34)$$

If the value of existed nodes in candidates of a node is less than the amount of privacy to share, that node is at risk of being identified.

Table (2) presents some information about recognizing database.

Table (2): candidates' size in the main set of data

شبکه	[۱/۱]	[۲/۹]	[۱۰/۱۹]	[۲۰/۴۹]	[۵۰/۱۰۰]
Polbook	7 %0.008	15 %0.020	18 %0.019	20 %0.025	28 %0.017
Maido	30 %185	55 %0.395	175 %0.245	215 %1.325	275 %1.109
Amazon	45 %0.065	255 %0.355	355 %0.315	425 %0.355	850 %0.265

Evaluation of the proposed method

In this section, the proposed method is evaluated. In the following sections, the particleFTV, MicroFTV and ModFTV algorithms were examined. All data sets presented in table (1) were used to evaluate the mentioned algorithms.

1-MicroFTV evaluation

MicroFTV algorithm was presented. In order to run the algorithm, we need each node to have a level of privacy. The data set in table (1) does not include this feature. This feature can be provided by the social network user. A normal distribution was used to assign a level of privacy to each node.

Table3: implementation time and the number in MicroFTV algorithm

network	$(h.g)$	time	$\vert C_g \vert$
Polbook	(10/10)	0:04:08	19856
	(20/10)	0:14:11	17562
	(50/20)	0:18:09	9635
	(100/50)	0:21:02	5362
Maido	(10/10)	0:00.09	66
	(20/10)	0:00.10	71
	(50/20)	0:00.13	61
	(100/50)	0:00.12	34
Amazon	(10/10)	0:00.09	2265
	(20/10)	0:00.10	3965
	(50/20)	0:00.12	652
	(100/50)	0:00.14	163

Received: 08 May 2025
Accepted: 07 February 2026

Table (3) is in 5 distribution levels which the valid number is between (1.5) which the higher the node's privacy requirement, the larger the number, and vice versa. Table (3) displays running time algorithm. It should be mentioned that as the size of $\omega -$ increases their number will decrease.

2- Evaluation of ModFTV

In ModFTV algorithm, firstly and if it is needed adding the edge or omitting the edge is done on the graph to equal the sum of sequence degree of shared r with the main graph. If it’s possible these changes will be done on those nodes which need changing temporal degree more than one time to achieve secure sharing. Then the algorithm will be done on the main graph to produce a suitable permutation and according to the d_G^* secured sequance degree is running.

It should be mentioned that$v$ *v1* must be in neighboring of *v3*but it must not be in neighboring of *v2.*

-The smallest path of η $(v1,\ v2)$ passes from v_3 and is passing from the shortest path among $(v_1,\ v_2)$ which is passing from the other neighbors is medial. This method is shown by η_{med}.

-The smallest path of η $(v1,\ v2)$ passes from v_3 and is passing from the shortest path among $(v_1,\ v_2)$ which is passing from the other neighbors is minimized. This method is shown by η_{min}

-The smallest path of η $(v1,\ v2)$ passes from $v_3$and is passing from the shortest path among $(v_1,\ v_2)$ which is passing from the other neighbors is maximized. This method is shown by η_{max}

Table 4_the results of ModFTV

network	η_G	$(h.g)$	f_3		
			η_{max}	η_{med}	η_{min}
Polbook	596.21×10^6	(10/10)	1256748	125658	63251458
		(20/10)	923584	1965358	56353225
		(50/20)	563257	2589674	45630258
		(100/50)	456328	4526895	36525129
Maido	235.63×10^6	(10/10)	6352	15632	13658
		(20/10)	6859	12563	63652
		(50/20)	6352	3256	189586
		(100/50)	1298	6539	-
Amazon	25.30×10^9	(10/10)	196588	358691	236595
		(20/10)	179585	263558	558965
		(50/20)	123658	325658	3652846
		(100/50)	569852	658352	129835

Table 4) the results of performance of ModFTV algorithm are shown. In this table the amount of η has shown the sum of the smallest path between two nodes in the main graph.

3) Evaluation of particleFTV algorithm

In this section sharing steps of the proposed algorithm are shown. According to the out put of the last section of CG particleFTV algorithm, has established a nearly optimum value as a sharing value for members. Medial presented results of the produced answers in 10 times performing algorithm are presented

Received: 08 May 2025
Accepted: 07 February 2026

for each series. The amount of population and the number of repetitions is established 50 and 100 respectively, which the number of summonses of seperation function is 4500 times in each performance. Also, the coefficient of a in relation (12-3) is established by the amount of 0.4 and 0.6 and 0.8. Table (5) shows the results of the experiments.

Table 5_ Results of performing particleFTV algorithm

	f_1	f_2	$(h.g)$	f		
				$\alpha = 0.4$	$\alpha = 0.6$	$\alpha = 0.8$
Polbook	0	85695	(10/10)	563255.3	4256.5	25895.8
	6	145896	(20/10)	735266.1	63524.5	4652369.3
	0	156985	(50/20)	186524.7	95263.7	428965.7
	0	198564	(100/50)	195632.5	15632.3	325698.6
Maido	0	125	(10/10)	124.3	138.2	75.7
	0	256	(20/10)	198.7	184.5	91.9
	19	459	(50/20)	352.9	412.5	158.4
	-	-	(100/50)	-	-	-
Amazon	8	7596	(10/10)	3698.2	458.4	3565.1
	0	74569	(20/10)	3598.6	2597.9	4125.4
	0	8965	(50/20)	4589.4	3258.4	3256.8
	5	75968	(100/50)	5625.3	6585.8	2652.7

In table 5 most of the amounts of summon functions of f_1 is equal to zero. It means the sum of sequance degree of the main graph and the graph of privacy are equal and the amount of density in both of the graphs are equal too. The amount of separation function of f_2 expresses how many temporal degree changes are needed in nodes for the main graph to become a secured graph for sharing.

Comparing the proposed method without personalization with other methods

In this section the results of proposed method are compared with two methods which presented by Geo et al. and Yang et al. these results are achieved from the method by Geo et al. [17] and Yang et al. [18]. Common data between all of the methods is Polbook data. For performance in the same condition MANTHK is used. Also, these methods are performed for these values k={1,2,3,4,5,6,7,8,9,10}. For all of the evaluations average error value is calculated which is shown by ε symbol. Table (6) is a summary of the results of comparison of MANTHK and other mentioned methods which the highlighted values represent the best result.

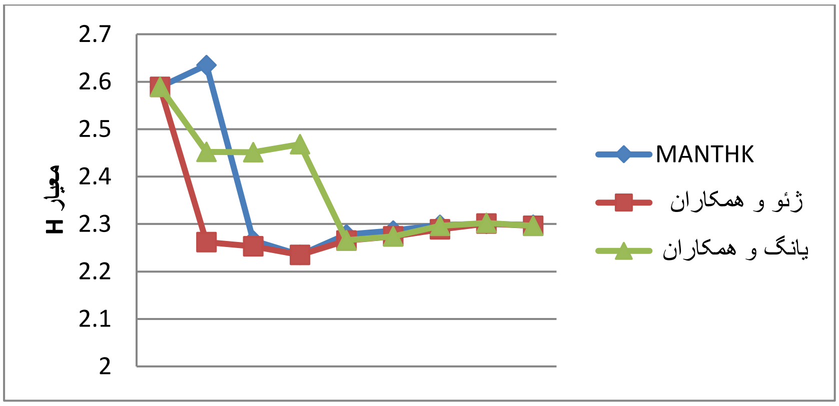
Table 6) comparison of proposed method with other methods

		K=1	K=2	K=3	K=4	K=5	K=6	K=7	K=8	K=9	K=10	ε
H	MANTH Zho K Yang	2.5896	2.635 2.362 2.452	2.265 2.253 2.451	2.235 2.235 2.468	2.278 2.265 2.266	2.286 2.274 2.267	2.296 2.289 2.274	2.298 2.296 2.296	2.300 2.301 2.302	2.298 2.296 2.296	0.012 0.285 0.39
D	MANTH Zho K Yang	0.325	0.265 0.265 0.219	.221 .220 .214	0.220 0.218	.220 0.218 0.21	0.220 0.219 0.214	0.220 0.217	0.224 0.219	0.223 0.220	0.221 0.218	0.007 0.009

					0.216	3		0.213	0.219	0.221	0.219	0.017
λ	MANTH Zho K Yang	22.025	40.8 41.09 -	41.35 42.37 -	45.19 46.16 -	45.24 46.26 -	45.19 46.18 -	45.18 46.21 -	45.21 46.26 -	45.22 46.24 -	45.36 46.41 -	0.185 1.137 -
T	MANTH Zho K Yang	37.43	38.35 38.35 44.05	38.19 35.19 44.16	39.11 39.19 45.20	39.15 36.09 44.17	39.18 39.18 44.17	39.22 39.21 44.26	39.26 39.24 44.23	39.22 39.24 44.20	39.21 39.18 44.31	0.009 0.006 4.236

1-Evaluation of the harmonic mean in the smallest distance

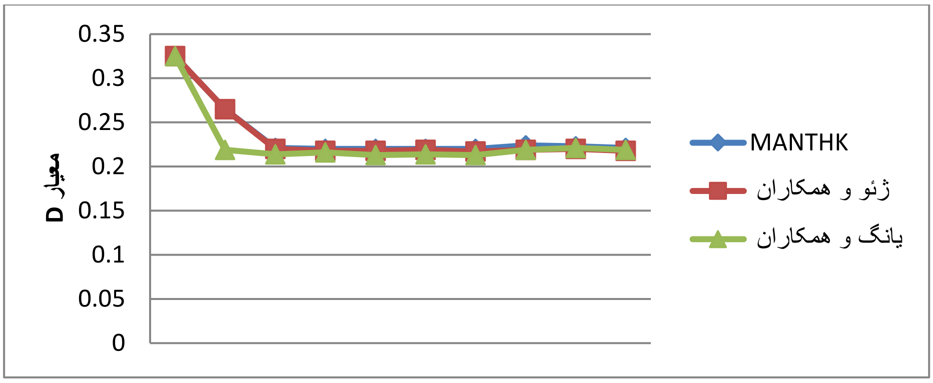
As it is mentioned in the previous section, this criterion is used to evaluate the connection in the social network graph. MANTHK method represented better results in evaluation of H criterion. The reason is optimization function that is considered in ModFTV section. This function tries to hold the value of the smallest path steady between two nodes and considers on H criterion on this feature. Geo's method uses only edge movement in the graph reconstruction which caused good results in this method. But in the method of Yang et.al because a node is added to the graph, this criterion includes more changes than those two initial methods.



Graph 1- evaluation of H criterion

2- Evaluation of density

graph (2) has shown evaluation of density criterion. This criterion is obtained from division of the number of existed edges in the graph rom the number of possible edges.

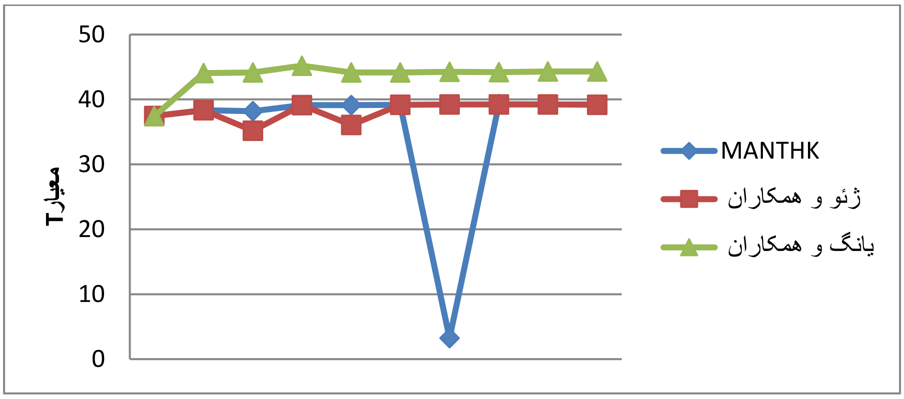


Graph 2- evaluation of D criterion

Both two methods of MANTHK Geo et al. and Yang et al try to hold amount of destiny steady. Therefore, they represent acceptable results. Although the method of Yang et al doesn’t add any edges to the graph and just secures the graph by changing the edge, but adding a node to the graph causes a lot of changes on the amount of density. Also, mean of the error on the two initial methods are very close to each other but the method of Geo et al. and Yang et al is less than MANTHK method.

3- Territorial evaluation

This method is used to evaluate local rings near to the node. Graph (3) shows the results of evaluation of this criterion.



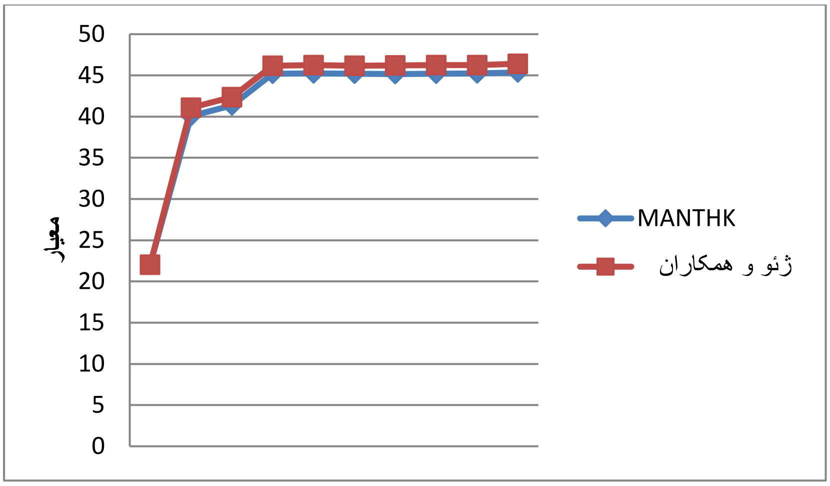
Graph 3- Evaluation of T criterion

Graph (3) shows that achieved results from MANTHK and Geo et al. and Yang et al methods are acceptable. Because of adding less howl to the graph like extra node and edge methods of MANTHK and Geo et al. and Yang et al maintain this feature better. However, the method of Yang et al., Despite not adding any extra edges, did not give acceptable results due to adding new nodes to the graph and changing the edges a lot.

4- evaluation of the most special amount in the matrix in neighboring of A

The special value contains information about the cycles available in the network. The more changes there are in the graph, the more this criterion changes. As it is mentioned, this value means the maximum value or $\lambda 1$. Figure (4) shows the results of this evaluation.

Received: 08 May 2025
Accepted: 07 February 2026



Graph 4- Evaluation of λ criterion

Graph 4 shows that MANTHK represents closer and better results than Geo et al. method. Both algorithms do not have a mechanism to keep this criterion fixed but due to the less changes in the proposed method in the social network graph, better results have been obtained. Also, error mean in the proposed method is lower and values of higher than k has less errors.

Comparison of the proposed method with other methods

In previous sections, the proposed method is considered without personalization with other previous methods. Results of the evaluation shows that MANTHK method provides similar level of privacy preserves the structural features of the network better. Therefore, in this part we compare the proposed method with MANTHK method on Polbook data series.

To do this, we evaluate two methods for the values k= {5,10}. We equaled δ values to 1 and 5 respectively. Results of the evaluation shows that MANTHK method preserves the structural properties of the network better than other methods of sharing. But a level of privacy for sharing which provides MANTHK is greater. In fact, this is the same compromise between privacy and usefulness of data.

Table (7) shows the value of privacy for provided sharing in two methods. Utilized criterion is disclosure risk which is expressed in chapter 3 and the smaller the number, the lower the risk of disclosure in sharing.

Table 7- disclosure risk for MANTHK method

	h=5 & g=1	h=10 & h=5
MANTHK	0.1148	0.0756

Table (7) shows that each node in social network is secured by some other nodes. Risk disclosure in sharing, in MANTHK and h=5 is equal to 0.1148 but if we vice versa this value represents that on average each node is secured by 0.0756 nodes. Therefore, the compromise between privacy and information usefulness is observed.

Conclusion

While social network and their users are increasing, existed data in social network increases. Whereas, the requirement of publishing data for research purposes can not be ignored. But publishing data jeopardizes privacy of efficiency in sharing. Although, preserving privacy in social network is in the first steps. Among developed method, sequence degree-based methods have better efficiency, because they preserve structural properties of social network better. In the methods that have been proposed so far for privacy in the social network and based on the sequence degree, the levels of privacy have been considered the same. In this thesis a method is proposed to preserve privacy in sharing social network of Instagram, which is based on the sequence degree and considered the requirements of privacy level of different users in social network of Instagram. This method includes three steps. In the first step the nodes are optimally placed in clusters in a micro-aggregation-based method, which ensures that the minimum amount of privacy is maintained for each node. In the second step, by maintaining the sum of the sequence degree and the least change in the graph, the amount of security for each node is determined. In the final step, if it's required first of all of the edges will be added to the graph or to omit it from the graph and then by displacement of edges, the graph is secured for sharing and is tried to constant the smallest path between two nodes. The results of this study are abreast with the results of Castantino et al. [19]. The MANTHK method was evaluated in Chapter 4 and compared with methods which attack the background knowledge of the degree of nodes. In comparison of this method with other methods on MicroFTV data series, the proposed method, regardless of the level of privacy of users in sharing on the social network Instagram, better preserves the structural features of the network. Though, all of the methods provide the same amount of privacy for the nodes. Then, at the end of the chapter the proposed method with personalization compared to a method without personalization and determined that if sharing of each person will be safe and secured according to his/her privacy requirements, then the usefulness of the data can be increased.

References

[1] R. Lu, X. Liang, X. Li, X. Lin, X.S. Shen, EPPA: an efficient and privacy-preserving aggregation scheme for secure smart grid communications, IEEE Trans. Parallel Distrib. Syst. 23(9) (2014) 1621–1631.

[2] H. Zhu, S. Du, M. Li, Z. Gao, Fairness-aware and privacy-preserving friend matching protocol in mobile social networks, IEEE Trans. Emerg. Top. Comput. 1(1) (2015) 192–200.

[3] G. Costantino, F. Martinelli, P. Santi, Privacy-preserving mobility-casting in op-portunistic networks, in: 2016 Twelfth Annual International Conference on Privacy, Security and Trust (PST), IEEE, 2014, pp.10–18.

[9] Yang, X, Lu,M, Liang,H. Tang,X.(2017), SFPM: A Secure and Fine-Grained Privacy-Preserving Matching Protocol for Mobile Social Networking, Journal of Big Data Research,1(8),1-8.

[10] Nettletona,D. Salas,J.(2018). A data driven anonymization system for information rich online social network graphs, Expert Systems With Applications, Expert Systems With Applications 251 (2017) 562–592.

[11] Zhao,K, Antonis C. Stylianou, Yiming Zheng,(2018), Sources and Impacts of Social Influence from Online Anonymous User Reviews, Journal OF Information an Managementhttp://dx.doi.org/10.1016/j.im.2017.03.006

[12] Yang, W., & Qiao, S. (2017). A 1454 novel anonymization algorithm: Privacy protection and knowledge preservation. Expert Systems with Applications, 37(1), 756–766 January 2017.

[13] Hansen, S.L., and Mukherjee, S.: 'A polynomial algorithm for optimal univariate microaggregation', IEEE Transactions on Knowledge and Data Engineering, 2014, 15, (4), pp. 1043-1044

[14] Machanavajjhala, A., Kifer, D., Gehrke, J., and Venkitasubramaniam, M.: 'l-diversity: Privacy beyond k-anonymity', ACM Transactions on Knowledge Discovery from Data (TKDD), 2017, 1, (1), pp. 3

[15] Newman, M.: 'Networks: an introduction' (Oxford University Press, 2013. 2014)

Received: 08 May 2025
Accepted: 07 February 2026

[16] Lewis, T.G.: 'Network science' (John Wiley & Sons, 2015. 2016)
[17] Freeman, L.C.: 'Centrality in social networks conceptual clarification', Social networks, 2014, 1, (3), pp. 215-239
[18] Costa, L.d.F., Rodrigues, F.A., Travieso, G., and Villas Boas, P.R.: 'Characterization of complex networks: A survey of measurements', Advances in Physics, 2016, 56, (1), pp. 167-242
94
[19] Bonacich, P.: 'Power and centrality: A family of measures', American journal of sociology, 2017, pp. 1170-1182
[20] Erd6s, P., and Rényi, A.: 'On the evolution of random graphs', Publ. Math. Inst. Hungar. Acad. Sci, 1960, 5, pp. 17-61
[21] Watts, D.J., and Strogatz, S.H.: 'Collective dynamics of 'small-world'networks', nature, 1998, 393, (6684), pp. 440-442
[22] Chung, F., and Lu, L.: 'Connected components in random graphs with given expected degree sequences', Annals of combinatorics, 2002, 6, (2), pp. 125-145
[23] Zheleva, E., Terzi, E., and Getoor, L.: 'Privacy in social networks', Synthesis Lectures on Data Mining and Knowledge Discovery, 2017, 3, (1), pp. 1-85
[24] Zheleva, E., and Getoor, L.: 'Privacy in social networks: A survey': 'Social network data analytics' (Springer, 2015), pp. 277-306
[25] Barbaro, M., Zeller, T., and Hansell, S.: 'A face is exposed for AOL searcher no. 4417749', New York Times, 2006, 9, (2014), pp. 8For
[26] Bhagat, S., Cormode, G., Krishnamurthy, B., and Srivastava, D.: 'Privacy in dynamic social networks','Book Privacy in dynamic social networks' (ACM, 2015, edn.), pp. 1059-1060
[27] Oganian, A., and Domingo-Ferrer, J.: 'On the complexity of optimal microaggregation for statistical disclosure control', Statistical Journal of the United Nations Economic Commission for Europe, 2014, 18, (4), pp. 345-353
[28] Domingo-Ferrer, J., and Torra, V.: 'A quantitative comparison of disclosure control methods for microdata', Confidentiality, Disclosure and Data Access: Theory and Practical Applications for Statistical Agencies, 2011, pp. 111-134
[29] Domingo-Ferrer, J., and Mateo-Sanz, J.M.: 'Practical data-oriented microaggregation for statistical disclosure control', Knowledge and Data Engineering, IEEE Transactions on, 2014, 14, (1), pp. 189-201
[30] Zhou, B., and Pei, J.: 'Preserving privacy in social networks against neighborhood attacks', 'Book Preserving privacy in social networks against neighborhood attacks' (IEEE, 2016, edn.), pp. 506-515
[31] Hay, M., Liu, K., Miklau, G., Pei, J., and Terzi, E.: 'Privacy-aware data management in information networks', 'Book Privacy-aware data management in information networks' (ACM, 2015, edn.), pp. 1201-1204
[32] Hay, M., Li, C., Miklau, G., and Jensen, D.: 'Accurate estimation of the degree distribution of private networks' 'Book Accurate estimation of the degree distribution of private networks' (IEEE, 2014, edn.), pp. 169-178